PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE

BILLS DIGEST

BILLS DIGEST NO. 49, 2018–19 3 DECEMBER 2018

Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Cat Barker and Helen Portillo-Castro
Foreign Affairs, Defence and Security Section
Monica Biddington
Law and Bills Digest Section

Contents

Date introduced: 20 September 2018

House: House of Representatives

Portfolio: Home Affairs

Commencement: Refer to page 11 of this Digest for details.

Links: The links to the Bill, its Explanatory Memorandum and second reading speech can be found on the Bill's home page, or through the Australian Parliament website.

When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the Federal Register of Legislation website.

All hyperlinks in this Bills Digest are correct as at December 2018.

ISSN 1328-8091

The Bills Digest at a glance

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 will amend a number of Acts—primarily the *Telecommunications Act 1997*, the *Australian Security Intelligence Organisation Act 1979* and the *Surveillance Devices Act 2004* (*SD Act*)—to facilitate access to certain communications and data for the purposes of disrupting and investigating criminal activity and threats to national security, including organised crime and terrorism.

The Government is responding to the impediment that the increasing prevalence of encrypted data and communications represents to available investigative and interception capabilities.

The Bill contains measures aimed at facilitating lawful access to communications and data through two avenues—decryption of encrypted technologies and access to communications and data at points where they are not encrypted.

Schedule 1 of the Bill will provide for industry assistance, which can be voluntary (a ***technical assistance request***) or ordered (a ***technical assistance notice*** or ***technical capability notice***). The industry participant is defined as a ***designated communications provider***, covering a broad range of persons and companies in the communications supply chain. The assistance provided by a designated communications provider would be in the form of technological assistance and include, but not be limited to: removing electronic protection; providing technical information; formatting information; and facilitating access to devices and other things.

The key amendments in **Schedule 2** of the Bill relate to ***computer access warrants***. These warrants permit covert access to data held in a target ***computer*** (which is broadly defined and may include more than one computer networks or systems). The amendments will:

- expand the powers available under computer access warrants and authorisations executed by the Australian Security Intelligence Organisation (ASIO), including by allowing ASIO to intercept a communication for the purpose of executing a computer access warrant and undertake activities to conceal access after the expiry of a warrant
- introduce equivalent computer access warrants for law enforcement agencies under the *SD Act* and
- make related amendments to the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979*.

Schedule 3 of the Bill will clarify and enhance the ability to collect evidence from electronic devices under warrant, by allowing the collection to occur remotely. Amendments will enable law enforcement to access information associated with an online or web-based account.

Schedule 4 of the Bill will bring the search warrant powers available to Australian Border Force (ABF) officers under the *Customs Act 1901* into closer alignment with those available to police under the *Crimes Act 1914*.

Both **Schedules 3** and **4** will expand the situations in which law enforcement officers may obtain an order requiring a person to provide assistance (such as authentication on a device), or risk a custodial sentence and/or a significant financial penalty.

Schedule 5 of the Bill will introduce civil liability protections for persons or bodies who, under certain circumstances, provide voluntary assistance at the request of the ASIO Director-General; or who make unsolicited disclosures to ASIO. This Schedule also introduces new coercive powers for ASIO under an assistance order regime, modelled on the regime available to law enforcement.

The Government released an Exposure Draft of the Bill and received a large number of submissions, largely focused on Schedule 1. The Bill has been referred to the Parliamentary Joint

Committee on Intelligence and Security for inquiry and report. Stakeholders have raised significant concerns about many aspects of the Bill, particularly Schedule 1. This Digest outlines the key provisions in the Bill and identifies many of the issues likely to be raised in the debate.

Purpose and structure of the Bill

The purpose of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) are as follows:

- **Schedule 1** will amend the *Telecommunications Act 1997* to allow or require industry to assist law enforcement and national security agencies to decrypt certain communications and make related amendments to the *Administrative Decisions (Judicial Review) Act 1977* (*ADJR Act*) and the *Criminal Code Act 1995* (*Criminal Code*).
- **Schedule 2** will:
  - amend the *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*) to expand the powers available under computer access warrants and authorisations executed by ASIO
  - amend the *Surveillance Devices Act 2004* (*SD Act*) to introduce computer access warrants for law enforcement agencies
  - make related amendments to the *Mutual Assistance in Criminal Matters Act 1987* and the *Telecommunications (Interception and Access) Act 1979* (*TIA Act*) and
  - amend the *TIA Act* to allow carriers to assist security authorities in activities relating to developing or testing technologies or interception capabilities.
- **Schedule 3** will amend the *Crimes Act 1914* to expand powers available to police under search warrant provisions so that they may:
  - compel a person specified in an assistance order to facilitate on the spot access to data held on a device found on a person that may hold evidential value to an investigation
  - access information associated with an online account and
  - access data remotely for the duration of the warrant.
- **Schedule 4** will amend the *Customs Act 1901* to expand powers available to ABF officials under search warrant provisions so that they may:
  - search persons
  - seek assistance orders that require a broader range of people who have a connection to a device to facilitate access to data that may hold evidential value to an investigation and
  - record fingerprints or take forensic samples from devices in possession of target persons.
- **Schedule 5** will amend the *ASIO Act* to introduce:
  - provisions for voluntary assistance to ASIO accompanied by a civil liability protection and
  - additional coercive powers for ASIO to require assistance in relation to its execution of a warrant authorised under existing provisions.

Key issues for debate

Key issues for debate in relation to **Schedule 1** of the Bill (**industry assistance**) include whether:

- the Bill should be amended to allow for judicial authorisation or oversight of the industry assistance scheme (page 24)
- the definition and scope of 'listed acts or things' is too broad and could be reduced in scope to prevent assistance that is not connected to a warrant (pages 24–25)
- a definition or further clarification can be inserted into the Bill on the terms 'systemic vulnerability' and 'systemic weakness' to address ambiguities raised by stakeholders (pages 26–27)
- the proposed penalties for failing to comply with a technology capability notice are proportionate to the gravity of the offence (page 30) and

- the Schedule should be passed in its current form, given the significant concerns and further recommendations for amendment from stakeholders including the Australian Human Rights Commission, the Inspector-General of Intelligence and Security, and technology and internet stakeholders (pages 15–16; 19–31).

Key issues for debate in relation to **Schedule 2** of the Bill (**computer access warrants**) include:

- whether telecommunications interception should be permitted for the purpose of executing a computer access warrant without a separate interception warrant (pages 33–36; 42)
- the breadth of the proposed powers to intercept communications, remove things from premises and conceal actions taken under a computer access warrant (pages 34–38; 42)
- whether improvements could be made to the safeguards and accountability mechanisms for the proposed expanded powers for the Australian Security Intelligence Organisation (ASIO) and new powers for law enforcement agencies (pages 35–38; 42; 47-50; 52–53)
- whether concealment actions should be permitted more than 28 days after the expiry of a warrant without further authorisation (pages 38; 42) and
- the breadth of the proposed assistance orders, and whether the proposed penalty for non-compliance is proportionate (pages 48–50).

Key issues for debate in relation to **Schedules 3** and **4** of the Bill (**search warrants and assistance orders—police and customs officer powers**) include whether:

- appropriate information handling and privacy safeguards are in place commensurate with the expansion of the information-gathering capability for law enforcement agencies (page 58) and
- the proposed amendments to the penalty regime for non-compliance with assistance orders are proportionate and adequately balance human rights and common law considerations (pages 56–58).

Key issues for debate in **Schedule 5** of the Bill (**voluntary or compulsory assistance to ASIO**) include whether:

- the scope of ***conduct*** that would constitute voluntary assistance is sufficiently defined, and whether an express provision pertaining to policy intent might provide a useful delimitation given **Schedule 1** amendments introducing technical assistance requests (pages 59–61)
- certain aspects of the assistance provisions may have unintended consequences for persons compelled or who volunteer to provide assistance; or for the rights of third parties—especially in a scenario of concurrent or consecutive use of ASIO's coercive powers (pages 59–62; 65–66) and
- explicit reporting, notification and record-keeping requirements would enhance oversight and accountability in relation to the actions ASIO undertakes and information it obtains through the use of voluntary or compelled assistance (pages 59–61; 66–67).

Background

The Bill contains significant measures that the Government argues are urgent and necessary to address the challenge law enforcement and intelligence agencies face in their investigations when presented with encrypted communications.[1] Maintaining lawful access to telecommunications content and data for national security and law enforcement purposes is a challenge with global

1. P Dutton, 'Second reading speech: Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018', House of Representatives, *Debates*, 20 September 2018, pp. 9671–74.

dimensions: the common problem faced by many governments and posed by the virtual ubiquity of encryption is known as 'going dark'.[2]

Telecommunications interception and access to telecommunications and other data are key investigative tools. Going dark refers to the impediment that the increasing prevalence of encrypted data and communications represents to available investigative and interception capabilities.[3] The issue has been understood as an eventual catalyst for legislative action for more than twenty years in Australia.[4] The extent of the challenge appears to be increasing. The proportion of internet communications intercepted by ASIO that were encrypted increased from three per cent in June 2013 to 55 per cent four years later.[5] Over 90 per cent of data intercepted by the Australian Federal Police (AFP) is now encrypted.[6]

The then Prime Minister, Malcolm Turnbull, first announced the legislative response embodied in the Bill as a priority in July 2017.[7] At that time, the then Attorney-General, George Brandis, stated:

> It is vitally important that the development of technology does not leave the law behind. … working with our international partners, in particular with our Five Eyes intelligence partners and with the broader global community … we will address this problem so as to keep our people safe. We will work with the corporate sector, we will engage them. It is an aspect of corporate social responsibility, which we will expect them to observe. But we'll also ensure that the appropriate legal powers, if need be, as a last resort, coercive powers of the kind that recently were introduced into the United Kingdom under the *Investigatory Powers Act*, or as long ago as 2013 were introduced in New Zealand under their *Telecommunications Act*, are available to Australian intelligence and law enforcement authorities as well.[8]

The Bill contains measures aimed at facilitating lawful access to communications and data through two avenues—decryption of encrypted material, and access to communications and data at points where they are not encrypted.

The Government's position is that the Bill should be passed quickly.[9] The Prime Minister and Minister for Home Affairs have called on the Parliamentary Joint Committee on Intelligence and Security (PJCIS) to expedite its inquiry to facilitate debate in both Houses during the final sitting fortnight of 2018.[10] As discussed elsewhere in this Bills Digest, stakeholders have raised concerns

---

2. J Lewis, D Zheng and W Carter, *The effect of encryption on lawful access to communications and data*, Center for Strategic and International Studies, Washington DC, 2017, pp. 12–17; M Burgess (Director-General, ASD), Evidence to Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Inquiry into Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, (proof), 19 October 2018, p. 5. For a summary of positions taken in the debate surrounding lawful access to encrypted content, see Internet Society and Chatham House, *Roundtable on Encryption and Lawful Access*, Chatham House, London, 26 October 2017.
3. The term appears to have been first coined in the United States. See for example: Federal Bureau of Investigation (FBI), *Going dark: law enforcement problems in lawful surveillance*, Cyber activity alert, FBI, 29 June 2011.
4. Attorney-General's Department (AGD), *The Walsh report: review of policy relating to encryption technologies*, AGD, Canberra, 1996.
5. Dutton, 'Second reading speech: Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018', op. cit. See also D Lewis, 'We need laws to disarm evildoers', *The Australian*, 10 October 2018, p. 12.
6. Ibid. See also A Colvin, 'Privacy not at risk as police seek tools to combat tech-savvy crims', *The Australian*, 20 September 2018, p. 12.
7. M Turnbull (Prime Minister) and G Brandis (Attorney-General), *Transcript of press conference: AFP Headquarters, Sydney*, media release, 14 July 2017.
8. Ibid.
9. 'Spying law push', *The West Australian*, 21 November 2018, p. 5; R Harris and A Galloway, 'Encryption laws to pass by end of year', *The Herald Sun*, 16 November 2018, p. 6; P Dutton (Minister for Home Affairs), Submission to Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 89], 22 November 2018.
10. S Morrison (Prime Minister), *Transcript of press conference with the Minister for Home Affairs, Sydney*, media release, 22 November 2018; P Dutton (Minister for Home Affairs), *Transcript of interview with Laura Jayes and Kieran Gilbert: First Edition, Sky News*, media release, 21 November 2018.

at the short time for consideration and questioned the necessity for the urgent passage of all or parts of the Bill.

Five Eyes nations: responses to 'going dark'

On 29 August 2018, a joint meeting was held between the Attorneys-General and Interior Ministers from the Five Eyes nations (Australia, Canada, New Zealand (NZ), the UK and the United States of America). The discussion about encryption and the problem of 'going dark' led to the agreement of a framework for discussion with industry to resolve the challenge 'while respecting human rights and fundamental freedoms'.[11]

This agreement was set out in the *Statement of Principles on Access to Evidence and Encryption*, affirming:

1. a mutual public safety responsibility between governments and technology providers that obliges assistance, while recognising the need to 'ensure the ability of citizens to protect their sensitive data'
2. the primacy of the rule of law and due process protections to ensure that 'lawful access should always be subject to oversight by independent authorities and/or subject to judicial review' and
3. '[f]reedom of choice for lawful access solutions' so that technology providers can 'voluntarily establish … customised solutions, tailored to their individual system architectures that are capable of meeting lawful access requirements'.[12]

The Bill was the first legislative proposal to have been tabled in any Five Eyes country since the Statement into which these principles might be read.[13] The UK and NZ have laws to oblige industry assistance with access to encrypted communications, whereas the United States and Canada have not amended existing provisions to impose comparable requirements on technology providers as yet.[14]

Exposure Draft consultation

Following earlier industry consultations, the Government released an Exposure Draft of the Bill on 14 August 2018 and sought public submissions by 10 September 2018.[15] The Department of Home Affairs (DoHA) received almost 16,000 submissions, of which over 15,000 were classified as standard campaign responses, 743 were 'unique individual responses classified as appropriate for consideration' and 55 were 'considered substantive submissions from industry groups, civil society, government bodies and individuals'.[16] While some stakeholders raised concerns about other schedules, the majority of submissions focused primarily or exclusively on Schedule 1 of the Exposure Draft (industry assistance).[17] Following the consultation, some changes were made to

---

11. Department of Home Affairs (DoHA), *Five Country Ministerial 2018: official communiqué*, media release, 30 August 2018, p. 3.
12. Five Country Ministerial/Quintet Meeting of Attorneys-General Australia 2018, *Statement of principles on access to evidence and encryption*, DoHA, 30 August 2018.
13. The question of whether the Bill might be regarded as model legislation for other nations is a matter of speculation in some of the commentary surrounding the proposed measures: see, for example, S Bradford Franklin, 'Looking down under for a back door', *Slate*, 5 October 2018.
14. The United Kingdom (UK) and New Zealand (NZ) laws were referred to in the then Attorney-General's July 2017 announcement about developing the Australian proposal (quoted above). See: *Investigatory Powers Act 2016* (UK) and *Telecommunications (Interception Capability and Security) Act 2013* (NZ).
15. DoHA, 'Consultations: the Assistance and Access Bill 2018', DoHA website; A Taylor (Minister for Law Enforcement and Cyber Security), *Public consultation commences on new Assistance and Access Bill*, media release, 14 August 2018.
16. DoHA, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 18], n.d., p. 41.
17. Ibid. Submissions for which consent was received to publish are available at: DoHA, 'Consultations: the Assistance and Access Bill 2018', op. cit.

Schedule 1 to respond to issues raised by industry and the public.[18] No changes were made to the other schedules.

Commencement details

Sections 1–3 of the Bill will commence on Royal Assent.

Part 1 of Schedule 1 will commence on proclamation, or nine months after Royal Assent, whichever occurs first. Part 2 of Schedule 1 will commence immediately after the commencement of Part 1 of Schedule 1 or immediately after the commencement of section 3 of the *Federal Circuit and Family Court of Australia Act 2018*, whichever occurs later; however, it will not commence at all if section 3 of the *Federal Circuit and Family Court of Australia Act* does not commence.[19]

Parts 1 and 2 of Schedule 2 and Schedules 3, 4 and 5 will commence the day after Royal Assent.

Part 3 of Schedule 2 will commence immediately after the commencement Part 1 of Schedule 2.[20]

Committee consideration

Parliamentary Joint Committee on Intelligence and Security

The Bill has been referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry and report. Details of the inquiry are at the inquiry homepage. Following a Government request to expedite its inquiry, the Chair and Deputy Chair of the Committee issued a statement pointing to the Committee's reviews of previous national security laws and stating that its reports had 'been carefully developed to ensure that new powers are proportionate and appropriately balanced with human rights and privacy, and that commensurate oversight and accountability is provided'.[21]

Some of the evidence presented to the PJCIS is included in the 'Position of major interest groups' and 'Key issues and provisions' sections of this Digest.

Senate Standing Committee for the Scrutiny of Bills

The Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) report, dated 18 October 2018, detailed concerns about several aspects of the Bill.[22] The Committee had concerns about each schedule of the Bill, and drew the attention of senators to concerns that fall across three general categories:

1. The breadth and significance of **powers conferred on the Executive** that may subsequently be subject to limited parliamentary scrutiny or oversight, specifically:
   - broad discretionary powers conferred under Schedule 1[23]
   - significant matters in delegated legislation under Schedule 1[24]
   - exclusion of judicial review of certain powers under Schedule 1[25]
   - broad delegation of administrative power under Schedule 2 and[26]

18. An overview of the changes is at Attachment H to DoHA's submission to the PJCIS: DoHA, Submission to PJCIS, op. cit., pp. 22–23. No changes were made to respond to issues raised in relation to other schedules of the Exposure Draft.
19. The Federal Circuit and Family Court of Australia Bill 2018 was before Parliament at the date of publication of this Digest.
20. Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* commenced on 22 November 2018.
21. PJCIS, *Joint statement by Chair and Deputy Chair*, media release, 22 November 2018.
22. Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee), *Scrutiny digest*, 12, 2018, The Senate, 17 October 2018, pp. 12–49.
23. Ibid., pp. 18–19 and pp. 26–27.
24. Ibid., pp. 16–17.
25. Ibid., pp. 22–23.

- coercive powers expanded or introduced under Schedules 2–5.[27]

2. The **impact on procedural fairness** where matters may be brought before the courts arising from the exercise of powers amended or introduced in the Bill, in particular:
   - reversal of the evidential burden of proof through the introduction of offence-specific defences under Schedule 1[28]
   - immunity from liability for the forms of assistance to law enforcement and intelligence agencies proposed under Schedules 1, 2 and 5[29]
   - significant penalties for failure to comply with assistance orders issued pursuant to amendments in Schedules 2–5 and[30]
   - the effect on the presumption of innocence arising from certificates issued under Schedules 2 and 5.[31]
3. The **privacy implications for individuals** of provisions in all schedules of the Bill, including the potential impact on the privacy of innocent third parties of provisions in Schedules 2–5.[32]

The Committee requested the Minister's advice on the above aspects of the Bill.

Following consideration of the Minister's response dated 12 November 2018, the Committee issued a second report on the Bill whereby it expressed residual concerns across all three categories and drew attention to these for the consideration of senators.[33] In particular, the Committee proffered suggestions to amend the Bill to:

- further limit powers conferred on the Executive
- address procedural fairness implications and
- mitigate privacy implications for individuals.[34]

The Committee also requested in its second report that a revised Explanatory Memorandum be tabled to include 'key information' contained in the Minister's response of 12 November.[35] In addition, the Committee drew certain matters to the attention of the Senate Standing Committee on Regulations and Ordinances.[36]

Further detail on issues raised by the Committee in its reporting on the Bill is included in the 'Key issues and provisions' sections of this Digest.

---

26. Ibid., pp. 27–28.
27. Ibid., pp. 28–42.
28. Ibid., pp. 25–27.
29. Ibid., pp. 23–25 (Schedule 1); pp. 47–49 (Schedules 2 and 5).
30. Ibid., pp. 45–47.
31. Ibid., pp. 42–45.
32. Ibid., pp. 20–21 (Schedule 1); pp. 35–39 and pp. 41–42 (Schedules 2–5).
33. Scrutiny of Bills Committee, *Scrutiny digest*, 14, 2018, The Senate, 28 November 2018, pp. 23–82.
34. Ibid.
35. Ibid. Requests to amend extrinsic materials with key information to aid legal interpretation are made as final comments for all of the concerns reiterated in this second report in relation to **Schedule 1**: see p. 33 (non-exhaustive definition of ***acts or things*** that may be specified in technical assistance requests); p. 34 (consultation obligations of the Minister with respect to **proposed subsection 317T(5)**); p. 37 (potential to use proposed **Schedule 1** framework in relation to minor offences or breaches of the criminal law); p. 40 (inclusion of foreign relations and national economic well-being under relevant objectives in **proposed subparagraph 317G(5)(d)** for issuing a technical assistance request); p. 42 (consultation obligations of the Minister with respect to **proposed section 317W**); p. 45 (exclusion of judicial review for decisions made under **proposed Part 15** of **Schedule 1**); p. 47 (extension of civil immunity to acts or things not exhaustively set out under **proposed section 317E**); p. 50 (offence-specific defences reversing evidential burden of proof proposed under **Schedule 1**); pp. 52–53 (compensation to providers in relation to technical assistance notices and technical capability notices under **proposed section 317ZK**). The Committee made such requests on pp. 57, 68 and 77 in relation to the privacy or other implications for third parties of provisions in **Schedules 2–5**.
36. Ibid., p. 35 (expansion of the definition of ***listed help*** by legislative instrument under **proposed subsection 317T(5)**) and p. 42 (no consultation obligation prior to a technical assistance notice being issued under **proposed section 317RA**).

Policy position of non-government parties/independents

Australian Labor Party

Labor reserved its position on the Bill until it considers the report and recommendations of the PJCIS.[37] The Government wrote to the PJCIS to request that it accelerate its consideration of the Bill to facilitate debate and passage in the Parliament.[38] However, the Opposition Leader, Bill Shorten, has said:

> It's an interesting point that government—this government who said every time it's all got to be rushed, there have been 300 amendments proposed to their 15 laws all of which have been accepted by the government. When you're dealing with terrorists and when you're dealing with national security and you're dealing with the rights of all Australians, rushing laws does not automatically make for good laws or effective laws. The worst thing that could happen is that the Government could propose a rushed law, someone is able to overturn it or undermine it and then the terrorists get off.[39]

On 30 November 2018, the Shadow Attorney-General wrote to the Attorney-General stating that the PJCIS had not reached bipartisan agreement on a report on the Bill:[40]

> Labor's commitment to the safety and security of Australians is unwavering, and will not be threatened by the Government's misbehaviour on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill*. But we will not be forced into a situation where the Parliament passes a bill that is unworkable and potentially weakens Australia's security.[41]

Labor has proposed that an interim Bill be passed to give federal agencies capabilities to enhance investigative capacity in relation to terrorist and child sex offences before Parliament rises for 2018. This would provide powers that agencies say are urgently required while giving the PJCIS more time to develop recommendations on the proposals in the Bill to empower state law enforcement bodies, given that the Commonwealth does not have oversight of those agencies.[42]

Australian Greens

The Greens have consistently expressed concerns about the Government's approach to legislating in this area. Senator Jordan Steele-John stated:

> This is massive government overreach and something we should all be extremely concerned about. It makes a mockery of our right to privacy, leaves us more vulnerable to cyber espionage and permanently weakens existing protections we all rely on to stay safe and secure online.[43]

Upon the Coalition party room's approval to introduce the Bill in the House of Representatives, Senator Steele-John expressed disappointment about the Government's level of engagement with

---

37. B Shorten (Leader of the Opposition), *Transcript of doorstop interview, Canberra*, media release, 26 November 2018.
38. Dutton, Submission to PJCIS, op. cit.
39. B Shorten (Leader of the Opposition), *Transcript of doorstop interview, Melbourne*, media release, 23 November 2018.
40. S Maiden (@samanthamaiden), 'Encryption fight: Labor's letter to Attorney-General confirming it will not pass all "flawed" laws by Christmas. This is the first time in a decade that the Joint Standing Committee on Intelligence Matters could not reach bipartisan approach' (includes photographs of the letter), tweet, 30 November 2018, https://twitter.com/samanthamaiden/status/1068357796905644032.
41. M Dreyfus (Shadow Attorney-General), Letter addressed to C Porter (Attorney-General), 30 November 2018 (attached to tweet cited above).
42. F Kelly, 'Interview with Mark Drefyfus', *RN Breakfast*, Australian Broadcasting Corporation (ABC), 3 December 2018. [Transcript unavailable at the time of publication of this Digest.]
43. J Steele-John, *Government approves introduction of anti- encryption bill without making public the consultation process*, media release, 18 September 2018.

submissions to the public consultation given that the announcement about the Bill's impending introduction came one week after that process closed.[44]

Other non-government parties and independents

Senator David Leyonhjelm (Liberal Democrats) has said 'The bill is a draconian measure to grant law enforcement authorities unacceptable surveillance powers that invade Australians' civil rights'.[45]

Senator Rex Patrick (Centre Alliance Party) has stated 'At the very least, equal attention should be paid to further strengthening oversight and accountability mechanisms to ensure that these powers are not abused'.[46]

Position of major interest groups

Many stakeholders raised concerns at the short times allowed for the public consultation on the Exposure Draft and consideration of the Bill by the PJCIS, and some questioned the necessity for the urgent passage of all or parts of the Bill.[47] An international digital rights advocacy group, Access Now, submitted that in order for Schedules 1 and 2 of the Bill to both be considered properly, they should be split into two separate Bills.[48]

The Australian Human Rights Commission (AHRC) suggested that the amendments made by the Bill should be reviewed by the Independent National Security Legislation Monitor and the PJCIS after three years to consider 'whether the policy objectives of the amendments remain valid and whether the new provisions have proven appropriate for securing those objectives'.[49] The Law Council of Australia (LCA) made a similar recommendation.[50]

As with the public consultation on the Exposure Draft, many of the submissions to the PJCIS's inquiry into the Bill focused solely or primarily on Schedule 1. Some of the main concerns are summarised briefly below. Further comment on the Bill from major interest groups is provided, where relevant, in the 'Key issues and provisions' sections of this Digest.

---

44. Ibid. See also: J Steele-John, *Government still can't explain how they plan to bypass encryption without compromising our online information*, media release, 6 June 2018.
45. D Leyonhjelm quoted in C Kruger, 'Spyware bill attracting privacy flak', *The Canberra Times*, 2 October 2018, p. 31.
46. R Patrick quoted in C Kruger, 'Spyware bill attracting privacy flak', op. cit.
47. See for example: Alliance for a Safe and Secure Internet, *Slow down, stop and listen – consumers, human rights groups, industry, telcos and technology companies join forces to sound alarm at Government's spyware legislation*, media release, 4 October 2018; Law Council of Australia (LCA), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 76], 18 October 2018, p. 6; Australian Industry Group (AiGroup), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 3], 10 September 2018, p. 1; Australian Communications Consumer Action Network (ACCAN), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 49], 12 October 2018, pp. 2–3; AHRC, Submission to DoHA, *Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 10 September 2018, p. 4.
48. Access Now, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 33], 12 October 2018, pp. 13–15. See also Office of the Victorian Information Commissioner (OVIC), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 45], 12 October 2018, p. 3 (arguing that the amendments to the *SD Act* in Schedule 2 should be subjected to substantial public debate).
49. Australian Human Rights Commission (AHRC), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 47], 12 October 2018, pp. 84–85.
50. LCA, Submission to PJCIS, op. cit., pp. 16–17.

Resource implications

The Inspector-General of Intelligence and Security (IGIS), who will oversee the use of new and expanded powers proposed for ASIO, the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD) stated:

> … the proposed amendments would increase considerably the scope and complexity of oversight arrangements and the workload of this Office. The adequacy of resourcing to maintain effective oversight would require ongoing monitoring and reassessment.[51]

The Commonwealth Ombudsman, who will oversee law enforcement agencies' use of computer access warrants, stated that the amendments to the *SD Act* in Schedule 2 are likely to substantially expand the office's oversight of powers under that Act, and stated that the office 'would welcome the opportunity to discuss additional resource requirements'.[52]

Penalties

Some stakeholders, including the Communications Alliance, the AI Group, Australian Information Industry Association (AIIA) and Australian Mobile Telecommunications Association (AMTA), raised concerns about the proposed penalties in Schedule 1 for failure to comply with notice provisions and disclosure offences.[53] In particular, they raised issues of compliance and enforcement of penalties particularly those not based in Australia:

> It is unclear how the Government plans to enforce the proposed legislation for [designated communications providers] with an overseas or trans-national presence. For example, if a large social media platform was issued a fine under the new legislation, it could withdraw operations, thereby reducing the range of services to which Australians have access, or simply refuse to pay. In such a scenario it is also questionable whether the level of fines of AUD 10 million would act as a sufficient deterrent given the global revenues of such companies.[54]

Schedules 2 and 5 will introduce new assistance orders and related offences, while Schedules 3 and 4 will amend the penalties for existing offences. Some stakeholders, including the AHRC and the LCA, questioned the proportionality of the penalties proposed for non-compliance with orders to provide assistance to ASIO and law enforcement agencies.[55]

Other key concerns about Schedule 1 (industry assistance)

Many stakeholders provided submissions that included general and specific recommendations on the proposed industry assistance scheme, including the IGIS, AHRC, LCA and applied cryptography academics Chris Culnane and Vanessa Teague.[56] There was significant concern that the scheme in

---

51. Inspector-General of Intelligence and Security (IGIS), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 52], 12 October 2018, p. 2.
52. Commonwealth Ombudsman, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 64], 15 October 2018, p. 4.
53. Communications Alliance, Australian Industry Group (AI Group), Australian Information Industry Association (AIIA) and Australian Mobile Telecommunications Association (AMTA), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 43], 12 October 2018, p. 20.
54. Ibid.
55. AHRC, Submission to PJCIS, op. cit., pp. 73–77; LCA, Submission to PJCIS, op. cit., p. 45.
56. IGIS, Submission to PJCIS, op. cit., pp. 6–39; AHRC, Submission to PJCIS, op. cit., pp. 20–58; LCA, Submission to PJCIS, op. cit. See also: BSA (Software Alliance), Submission to DoHA, *Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 10 September 2018, pp. 5–13; Internet Australia, Submission to DoHA, *Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 10 September 2018, pp. 6–10; Coalition of Civil Society Organisations & Technology Companies & Trade Associations, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 29], 11 October 2018; C Culnane and V Teague, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 16], September 2018, pp. 11–12.

its current form has a very wide application and that amendments to offer greater definition, narrow the scope or clarify processes are necessary.

From a technology perspective, Apple submitted that Schedule 1 'remains dangerously ambiguous with respect to encryption and security'.[57] Further, Apple stated:

> We encourage the government to stand by their stated intention not to weaken encryption or compel providers to build systemic weaknesses into their products. Due to the breadth and vagueness of the Bill's authorities, coupled with ill-defined restrictions, that commitment is not currently being met. For instance, the Bill could allow the government to order the makers of smart homespeakers to install persistent eavesdropping capabilities into a person's home, require a provider to monitor health data of its customers for indications of drug use, or require the development of tool that can unlock a particular user's device regardless of whether such [a] tool could be used to unlock every other user's device as well… While we share the goal of protecting the public and communities, we believe more work needs to be done on the Bill to iron out the ambiguities on encryption and security to ensure that Australian are protected to the greatest extent possible in the digital world.[58]

Other key concerns about Schedules 2–5 (computer access warrants, expanded search powers, and assistance orders)

The IGIS, Commonwealth Ombudsman, AHRC and LCA raised concerns about several aspects of the expanded computer access warrant powers for ASIO and new computer access warrants for law enforcement agencies in **Schedule 2**, including:

- the appropriateness of permitting telecommunications interception for the purpose of executing a computer access warrant; and if it is to be permitted, the breadth of the proposed power
- the breadth of the proposed powers to remove things from premises and conceal actions taken under a computer access warrant (including after a warrant has expired)
- how information obtained through intercepting a communication for the purpose of executing a warrant will be dealt with and
- the adequacy of safeguards and accountability mechanisms.[59]

Some stakeholders were concerned about the possible impact of the proposed orders in **Schedule 2** to provide assistance with the execution of a computer access warrant on the privilege against self-incrimination.[60] This concern was also raised in relation to assistance orders introduced or amended by **Schedules 3–5**.

---

57. Apple, Inc., Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 53], n.d., p. 2.
58. Ibid. See also: Information Technology Professionals Association, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 37], 12 October 2018; Australian Information Security Association, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 40], 11 October 2018; ACCAN, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, op. cit.
59. IGIS, Submission to PJCIS, op. cit., pp. 39–51; IGIS, Supplementary submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 52.1], 23 November 2018, pp. 2–6; Commonwealth Ombudsman, Submission to PJCIS, op. cit., pp. 4–7; AHRC, Submission to PJCIS, op. cit., pp. 58–73; LCA, Submission to PJCIS, op. cit., pp. 33–44, 47.
60. LCA, Submission to PJCIS, op. cit., pp. 45–47; AHRC, Submission to PJCIS, op. cit., pp. 77–80; D Hochstrasser, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 61], October 2018, pp. 1–3; Australian Privacy Foundation, Digital Rights Watch, Electronic Frontiers Australia, Future Wise, Access Now, Blueprint for Free Speech and Getup! (listed as Civil Society), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 55], October 2018, p. 33.

The President of the Senate wrote to the PJCIS, the Attorney-General and the Minister for Home Affairs to raise concerns about the interaction of computer access warrants under the *SD Act* (**Schedule 2**) and expanded search powers in the *Crimes Act* and *Customs Act* (included in **Schedules 3** and **4** of the Bill respectively) with parliamentary privilege.[61]

Financial implications

The Explanatory Memorandum states that financial impacts of the Bill will be met from existing appropriations.[62]

The Explanatory Memorandum does not contain an estimate of the possible financial impact of the measures in the Bill or potential regulatory costs on industry. AustCyber (a government-backed cyber security industry initiative to assist Australian businesses in that sector) and the Australian Strategic Policy Institute have jointly conducted a survey for the sector about the economic impact of the Bill on industry.[63] At the time of publication of this Digest, a report on the survey was expected to be released during the final sitting week for 2018.

Statement of Compatibility with Human Rights

As required under Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth), the Government has assessed the Bill's compatibility with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of that Act. The Government considers that the Bill is compatible.[64]

Parliamentary Joint Committee on Human Rights

The Parliamentary Joint Committee on Human Rights (PJCHR) considered that there are questions about whether parts of the Bill are compatible with certain human rights.[65] The PJCHR's 47-page analysis found that various aspects of the Bill engage and may limit a number of human rights, including in ways not addressed in the statement of compatibility.

The analysis highlighted 10 aspects of the Bill relating to measures in different Schedules.[66] The right to privacy featured heavily in the PJCHR's comments, which revolved principally around the proportionality or compatibility of measures in relation to this right. Another frequently cited concern related to potential limitations on an individual's ability to seek legal recourse where they may be affected by actions pursuant to one of the proposed measures, through engaging either the right to a fair trial and fair hearing or the right to an effective remedy. Additional concerns were raised with respect to other rights under relevant treaties.

Table 1 shows measures that the PJCHR commented upon and—while noting the statement of compatibility had acknowledged the engagement of certain rights in several instances—sought the Minister's advice to address concerns raised in its report. Measures are listed in order of the

---

61. S Ryan (President of the Senate), Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 94], 27 November 2018.
62. Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, p. 7.
63. S Sharwood, 'Cyber industry probes economic impact of crypto bill', *IT News*, 23 November 2018; D Sadler, 'AustCyber report on encryption bill', *InnovationAus.com*, 28 November 2018.
64. The Statement of Compatibility with Human Rights can be found at page 8 of the Explanatory Memorandum to the Bill.
65. Parliamentary Joint Committee on Human Rights (PJCHR), *Human rights scrutiny report*, 11, 16 October 2018, pp. 24–71.
66. Whereas the PJCHR commented on certain measures in its report, other stakeholders have raised concerns about the engagement and potential limitation of human rights in relation to other measures, or other human rights in relation to the same measures as those identified by the PJCHR. This Digest does not present an analysis of overlapping concerns, or provide a summary of overall concerns, but indicates stakeholder views under the 'Key issues and provisions' sections and other headings.

Schedule in which they appear, and which rights the PJCHR considered to be engaged and potentially limited through provisions in the Bill.

Table 1: Summary of PJCHR's analysis of rights engaged and potentially limited by measures

Schedule	Measure	Fair trial/hearing and/or effective remedy	Privacy	Other right under relevant treaty*
Schedule 1	Technical assistance notices and requests, and technical capability notices[67]	Y	Y	Freedom of expression
Schedules 2–5	Powers to compel persons to assist officers to access data and devices[68]	N	Y	—
Schedule 2	Computer access warrant scheme[69]	Y	Y	Right to life Freedom from torture, cruel, inhuman and degrading treatment or punishment (through the use of force power) (See also comments concerning the interaction of amendments with control orders regime.)
Schedule 2	Interception of communications through computer access warrants[70]	N	Y	—
Schedule 2	Concealment of access power[71]	N	Y	—
Schedule 2	Assistance to foreign countries in	Y	N	Right to liberty Right to life

67. Ibid., pp. 27–40.
68. Ibid., pp. 54–57.
69. Ibid., pp. 40–51.
70. Ibid., pp. 58–61.
71. Ibid., pp. 51–54.

Schedule	Measure	Fair trial/hearing and/or effective remedy	Privacy	Other right under relevant treaty*
	relation to data held in computers[72]			Prohibition against torture and cruel, inhuman and degrading treatment Right to equality and non-discrimination
Schedules 3 and 4	Power for police and Australian Border Force to access computers remotely[73]	N	Y	—
Schedules 3 and 4	Amendments to allow electronic devices moved under warrant to be kept for analysis for 30 days[74]	N	Y	—
Schedule 4	Power for Australian Border Force to search persons who may have computers or devices[75]	N	Y	—
Schedule 5	Release from civil liability for providing voluntary assistance to ASIO[76]	Y	N	—

Source: Parliamentary Joint Committee on Human Rights (PJCHR), *Human rights scrutiny report*, 11, 16 October 2018, pp. 24–71.

Notes:

* The PJCHR makes an assessment of legislation against human rights contained in the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD); the International Covenant on Economic, Social and Cultural Rights (ICESR); the International Covenant on Civil and Political Rights (ICCPR); the Convention on the Elimination of Discrimination against Women (CEDAW); the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT); the Convention on the Rights of the Child (CRC); and the Convention on the Rights of Persons with Disabilities (CRPD).

The Minister's response had not been published by the PJCHR as at the date of publication of this Digest.

72. Ibid., pp. 61–64.
73. Ibid., pp. 64–67.
74. Ibid., pp. 69–70.
75. Ibid., pp. 67–69.
76. Ibid., pp. 70–71.

Industry assistance: key issues and provisions in Schedule 1

Schedule 1 will introduce a tiered approach for designated communications providers that undertake eligible activities to provide assistance to law enforcement and national security agencies.

Immunity from criminal liability

Items 2 and **3** of **Schedule 1** to the Bill will amend the *Criminal Code* by inserting **proposed subsection 474.6(7A)** and **proposed subparagraphs 476.2(4)(b)(iv)-(vi)** to protect designated communications providers from criminal liability in relation to one telecommunications services offence (section 474.6(5) of the *Code*) and all computer offences in Part 10.7 of the *Code* where they are acting in accordance or compliance with a technical assistance request or notice, or technical capability notice.

Industry assistance under the Telecommunications Act

Item 7 of **Schedule 1** proposes to insert new *Part 15—Industry Assistance* into the *Telecommunications Act*, which will allow law enforcement and national security agencies to request or require ***designated communications providers*** to provide assistance.

Definitions

Proposed Part 15 of the *Telecommunications Act* is comprised of **proposed sections 317A to 317ZT**.

The new definitions section in **proposed section 317B** explains key terminology, including:

- ***access***, which, when used in relation to material, will include access that is subject to a precondition (for example, a password), access by way of push technology and access by way of a standing request
- ***designated communications provider*** will have the meaning given by **proposed section 317C** (discussed below)
- ***giving help*** will include giving help to an employee, affiliate or staff member of the relevant agency (ASIO, ASIS, ASD or law enforcement body)
- ***interception agency*** will mean the 17 agencies listed, including all state police forces and the crime and corruption commissions in NSW, Victoria, Queensland, South Australia and Western Australia
- ***material*** will mean material in the form of text, data, speech, music or other sounds, visual images (moving or otherwise), or any other form or combination of forms
- ***supply***, when used in relation to a facility, customer equipment or a component, will include supply by way of sale, exchange, lease, hire or hire-purchase and, in relation to software includes provide, grant or confer rights, privileges or benefits.[77]

Measures to allow law enforcement and security agencies to secure assistance

Proposed Part 15 of the *Telecommunications Act* will outline the details of a tiered approach for a designated communications provider who undertakes eligible activities to provide assistance to law enforcement and national security agencies.[78]

A ***designated communications provider*** will be broadly defined in the table in **proposed section 317C** and will include:

77. See **proposed section 317B** for the full list of definitions.
78. **Proposed section 317C**.

- a carrier or carriage service provider (item 1 of the table in **proposed section 317C**)[79]
- a person who provides an electronic service (defined in **proposed section 317D** as a service that allows end-users to access material using a carriage service or a service that delivers material to people through a carriage service) (item 4 of the table)
- a person providing a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia (item 5 of the table)
- a person who develops, supplies or updates software used in connection with a listed carriage service or an electronic service with end-users in Australia (item 6 of the table) and
- a person who manufactures, supplies, installs, maintains or operates telecommunications infrastructure (item 7 of the table).

The breadth of this definition means that it will apply to diverse people and entities, from multinational corporations such as Facebook, large Australian companies such as Telstra, to individuals such as a Telstra technician or retail repairer. The Explanatory Memorandum states that the definition 'is crafted in technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves'.[80] However, the Communication Alliance noted that the definition meant that assistance could be required to be provided in 'almost any circumstance anywhere in the supply chain'. [81]

The DIGI submission further states that 'this [definition] allows Notices to be issued to companies anywhere in the supply chain of a provider, requiring the companies to build and provide compromised or vulnerable software, equipment or services to the service providers without the service provider's knowledge. This is an untenable position for any service provider'.[82]

Assistance from a designated communications provider may be requested or required through:

- a ***technical assistance request*** (TAR) (**Division 2 – Voluntary technical assistance**)
- a ***technical assistance notice*** (TAN) (**Division 3 – Technical assistance notices**) or
- a ***technical capability notice*** (TCN) (**Division 4 – Technical capability notices**).

Technical assistance request (TAR)

A TAR is a request from the head of ASIO, ASIS, or ASD, or the chief officer of an ***interception agency*** to a designated communications provider, asking the provider voluntarily to do specified acts or things directed towards ensuring that the provider is capable of giving help to the requesting agency in relation to the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a state or territory that relates to:

- enforcing the criminal law and laws imposing pecuniary penalties
- assisting the enforcement of the criminal laws in force in a foreign country or

---

79. Carriers are defined as those persons who own a telecommunications network unit that is used to supply carriage services to the public. A carriage service provider (CSP) uses, but does not own, a telecommunications network unit to provide carriage services to the public. A CSP can include organisations that resell time on a carrier network for phone calls, provide access to the internet (internet service providers or ISPs) or provide telephone services over the internet (VoIP service providers). CSPs do not require a licence to supply a carriage service to the public. See, Australian Communications and Media Authority (ACMA), *Know your obligations: carriers and carriage service providers, including internet and VoIP service providers*, ACMA, September 2015, p. 2.
80. Explanatory Memorandum, p. 35.
81. Communications Alliance, AIIA and AMTA, Submission to DoHA, *Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 7 September 2018, p. 14.
82. Digital Industry Group Inc (DIGI) Submission to PJCIS *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 78], p. 4.

- the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.[83]

A TAR may also cover matters that facilitate, or are ancillary or incidental to, such matters.[84]

The acts or things that may be specified in a TAR include (but are not limited to) ***listed acts or things*** provided that they are in connection with any of the eligible activities of the particular designated communications provider (as set out in the table in **proposed section 317C**). ***Listed acts or things*** include removing electronic protection, providing technical information, installing software, putting information in a particular format and facilitating access to devices or services (**proposed section 317E**).

Significant concerns about the ability to request assistance from a designated communications provider for the enforcement of any Commonwealth, state or territory criminal law and laws imposing pecuniary penalties, and assisting the enforcement of foreign criminal laws, were noted by the Scrutiny of Bills Committee. This objective may allow a large number of agencies to use the proposed framework to request or require providers to do certain acts or things when investigating or prosecuting even very minor offences or breaches of the law subject to a pecuniary penalty.[85] The Committee stated:

> … it therefore appears that the proposed framework is not limited to investigating only serious offences relating to organised crime, terrorism, smuggling, and sexual exploitation of children, as identified in the explanatory memorandum.[86]

Technical assistance notice (TAN)

A TAN differs from a TAR in that it requires (rather than requests) a designated communications provider to do specified acts or things to assist the issuing agency to perform functions or exercise power in relation to:

- enforcing the criminal law and laws imposing pecuniary penalties
- assisting the enforcement of the criminal laws in force in a foreign country or
- safeguarding national security.[87]

A TAN may also cover matters that facilitate, or are ancillary or incidental to, such matters.[88]

A TAN may be issued by the head of ASIO or the chief officer of an interception agency.[89] A TAN must not be issued unless the head of ASIO or the chief officer of an interception agency (as relevant) is satisfied that the requirements of the notice are reasonable and proportionate, and compliance with the notice is both practicable, and technically feasible (**proposed section 317P**).

In considering whether the requirements imposed by a TAN are reasonable and proportionate, the Director-General of Security or the chief officer of an interception agency must have regard to the interests of national security and law enforcement; the legitimate interests of the designated communications provider to whom the notice relates; the objectives of the notice; the availability of other means to achieve the objectives of the notice; the legitimate expectations of the

---

83. **Proposed subsection 317G(5)**. These are referred to as the **relevant objectives**. See further, Explanatory Memorandum, pp. 44–45.
84. **Proposed subparagraph 317G(2)(a)(vi)**.
85. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., pp. 18–19.
86. Ibid.
87. **Proposed subsection 317L(2)**.
88. **Proposed paragraph 317L(2)(d)**.
89. **Proposed subsection 317L(1)**.

Australian community relating to privacy and cybersecurity and any other relevant matters (**proposed section 317RA)**.

Technical capability notice (TCN)

A TCN is issued by the Attorney-General (**proposed section 317T**) in writing and requires a provider to *build a new capability* that will enable them to give assistance to ASIO or interception agencies, where the Attorney-General is satisfied that the requirements are 'reasonable and proportionate' and that compliance is 'practicable and technically feasible' (**proposed section 317V**). In considering whether the requirements in a TCN are 'reasonable and proportionate' the Attorney-General must have regard to:

- the interests of national security and law enforcement
- the legitimate interests of the designated communications provider to whom the notice relates
- the objectives of the notice
- the availability of other means to achieve the objectives of the notice
- the legitimate expectations of the Australian community relating to privacy and cybersecurity and
- any other relevant matters (**proposed section 317ZAA**).

The Explanatory Memorandum provides:

> This means the decision-maker must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate, it is necessary for the decision-make to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider…
>
> The decision-maker must also consider wider public interests, such as any impact of privacy, cyber security and innocent third parties… These provisions are designed to ensure that provider cannot be required to comply with excessively burdensome or impossible assistance measures.[90]

The TCN can require the provider to do one or more specified acts or things:

- directed towards ensuring that the provider is capable of giving help to or
- giving help to

the requesting agency in relation to the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a state or territory that relates to:

- enforcing the criminal law and laws imposing pecuniary penalties
- assisting the enforcement of the criminal laws in force in a foreign country or
- safeguarding national security.[91]

A TCN may also cover matters that facilitate, or are ancillary or incidental to, such matters.[92]

The Attorney-General must consult the provider and consider any submission by the provider before issuing a TCN (**proposed section 317W**).

---

90. Explanatory Memorandum, p. 49.
91. **Proposed subsection 317T(3)**.
92. **Proposed subparagraphs 317T(2)(a)(ii)** and **317T(2)(b)(ii)**.

The TCN may have a specified duration, and if it does not, it will expire at the end of 180 days after issue (**proposed section 317U**). It can be varied by the Attorney-General (**proposed section 317X**) after consultation with the provider (**proposed section 317Y**).

The IGIS will oversee the involvement of ASIO, ASD and ASIS in initiating and administering TARs, and the actions of ASIO in issuing and administering TANs and making any requests to the Attorney-General for TCNs.

Proposed section 317ZK provides that, unless the relevant agency head (in the case of TANs) or the Attorney-General (in the case of TCNs) decides that it would be contrary to the public interest, the designated communications provider is required to comply with the notice on the basis that the provider will neither profit from that compliance nor bear the reasonable costs of such compliance. Different costs arrangements can also be agreed between the provider and the applicable costs negotiator (which is the relevant agency head in the case of TANs or the person specified in the TCN).[93] In relation to the ability to decide that the costs of complying with a notice will not be recoverable, the Explanatory Memorandum states:

> In some circumstances it will not be appropriate to compensate a provider subject to a notice, for example where it has been issued to remediate a risk to law enforcement or security interests that has been recklessly or wilfully caused by a provider. [94]

However, **proposed section 317ZK** has no effect to the extent to which it would result in an acquisition of property otherwise than on just terms under paragraph 51(xxxi) of the *Constitution* (**proposed subsection 317ZK(15)**).

The Scrutiny of Bills Committee requested further detailed advice from the Minister as to the circumstances where it would not be appropriate to compensate a provider that is subject to a TAN or TCN. Further, the Committee sought advice as to 'why (at least high level) guidance' could not be included in the Bill on the circumstances in which **proposed section 317ZK** will not apply.[95]

Issue: Judicial authorisation should determine need for industry assistance

Some stakeholders considered that the decision to issue a notice should be made by an independent judicial authority on the basis of evidence and an assessment of clear criteria.[96] This is particularly the case when significant penalties apply for a failure to comply with a TAN or TCN to the extent that the provider is capable of doing so:

> Industry recommends, at the very minimum, that consideration be given to the establishment of a specific judicial oversight regime, and possibly the introduction of an Investigatory Powers Commissioner, similar to the measures included in the UK *Investigatory Powers Act 2016*. This will also help with aligning the legislation better with Australia's obligations under the Budapest Convention on Cybercrime.[97]

Further, the LCA expressed concern at the absence of independent judicial review and said that with 'little transparency as to the frequency and nature of use of these measures, there may be a

93. **Proposed subsection 317ZK(16)**.
94. Explanatory Memorandum, op. cit., p. 71.
95. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., p. 26.
96. Digital Industry Group Inc (DIGI), Submission to DoHA, *Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, op. cit., p. 5.
97. Communications Alliance, AIIA and AMTA, Submission to PJCIS, op. cit., p. 19.

risk that this Bill (if enacted in its current form) will result in erosion of digital trust of citizens in activities of intelligence and law enforcement agencies'.[98]

Listed acts or things

A TAR, TAN or TCN may request (in the case of a TAR) or require (in the case of a TAN or TCN) the provider to do one or more 'specified acts or things'. These acts or things may include (but are not limited to) ***listed acts or things*** (defined in **proposed section 317E**). The list is extensive and is well explained in the Explanatory Memorandum, including that:

- **proposed paragraph 317E(1)(a)** 'removing one or more forms of electronic protection' is intended to include decrypting encrypted communications. This does not then oblige the provider to 'furnish the content or metadata of private communications to authorities' and
- 'providing technical information' includes design, manufacture, creation or operation of a service, the characteristics of a device, or matters relevant to the sending, transmission, receipt, storage or intelligibility of a communication (**proposed paragraph 317E(1)(b)**).[99]

The IGIS noted that 'several "listed acts or things" appear to be acts of things for which ASIO would, or may depending of the facts, require a warrant or an authorisation to undertake itself'.[100]

In relation to **proposed paragraph 317E(1)(b)**, which includes 'providing technical information' as one of the ***listed acts or things***, the Communications Alliance noted that while 'technical information' is an undefined term in the Bill, the Explanatory Memorandum provides some examples of what technical information could include and notes source code. The Communications Alliance submitted that 'obtaining source code and information that may reveal vulnerabilities is not necessary or reasonable for the purpose of law enforcement and does not comply with the principle of proportionality'.[101]

The Scrutiny of Bills Committee also expressed concern that the acts or things that may be requested or required are not limited to the listed acts or things under **proposed section 317E**. The Committee stated that the Explanatory Memorandum 'does not provide a justification as to why it is necessary to allow a technical assistance request or a technical assistance notice to specify acts or things beyond those acts or things listed in proposed section 317E'.[102]

Definition of technical information

As discussed above, **proposed paragraph 317E(1)(b)** will list 'providing technical information' as an act or thing that may be specified in any of the requests or notices. The term 'technical information' is not defined in the Bill. The Explanatory Memorandum states that this term 'could include information about the design, manufacture, creation or operation of a service, the characteristics of a device, or matters relevant to the sending, transmission, receipt, storage or intelligibility of a communication'. It lists examples including source code, network or service design plans, and the details of third party providers contributing to the delivery of a communications service, the configuration setting of network equipment and encryption schemes.[103]

98. LCA, Submission to PJCIS, op. cit., p. 7.
99. Explanatory Memorandum, p. 39.
100. IGIS, Submission to PJCIS, op. cit., p. 10.
101. Communications Alliance, AIIA and AMTA, Submission to PJCIS, op. cit., pp. 17–18.
102. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., p. 15.
103. Explanatory Memorandum, p. 39.

The Explanatory Memorandum does clarify that technical information does not include telecommunications data such as subscriber details or the source, destination or duration of a communication for which an authorisation under the *TIA Act* would be required.[104]

This is another example of a term that could be interpreted very broadly, potentially encroaching on circumstances where a warrant authorisation should be required.

Listed help

Under a TCN, the Attorney-General may require a provider to do specified things that are connected to the eligible activities of the provider[105] and either:

- are directed to ensuring that the provider is capable of giving ***listed help*** to ASIO or the relevant interception agency or
- give help to ASIO or the relevant interception agency (**proposed subsection 317T(2)**).

This means that a direction from the Attorney-General requiring a provider to *develop a capability* that can be used to assist security or law enforcement agencies can only relate to the provision of ***listed help***.

Proposed subsection 317T(4) provides that listed help is an act or thing done by a provider:

- by way of giving help to ASIO or an interception agency
- in connection with any or all of the eligible activities of the provider[106] and
- which consists of either or both of:
  - one or more of the ***listed acts or things*** (in **proposed section 317E**), other than removing a form of electronic protection
  - an act or thing determined by the Minister through a legislative instrument.[107]

If the Minister makes a determination of an act or thing that is ***listed help*** (as allowed under **proposed subsection 317T(5)**), he or she must have regard to the interests of law enforcement; the interests of national security; the objects of the Act; the likely impact of the determination on designated communication providers and any other matters as the Minister considers relevant (**proposed subsection 317T(6)**).

The Explanatory Memorandum notes that the legislative instrument making power allows the Minister to list further areas with respect to which capabilities under a notice may be built, additional to the listed acts or things in **proposed section 317E**. However, it also creates uncertainty as to how the powers in the Bill will be applied in the future. The AHRC recommended that **proposed subsection 317T(5)** be removed, to prevent the expansion of the definition of 'acts or things' for the purposes of a TCN by way of legislative instrument.[108]

The Scrutiny of Bills Committee considered that a sound justification for the use of delegated legislation should be provided, particularly where compliance with the notices is subject to a civil penalty of up to $10 million (see discussion of penalties below).[109]

---

104. Ibid.
105. Listed in **proposed section 317C**.
106. See column 2 of the table at **proposed section 317C**.
107. The legislative instrument may be made under **proposed subsection 317T(5)**.
108. AHRC, Submission to DoHA, op. cit., pp. 21–23.
109. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., p. 16.

Issue: Undefined 'systemic weakness' and 'systemic vulnerability'

Proposed section 317ZG lists a key limitation for designated communications providers. That is, that a TAN or TCN must not have the effect of requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection, and must not prevent the provider from rectifying such a weakness or vulnerability. The Explanatory Memorandum describes:

> … if an agency were undertaking an investigation into an act of terrorism and a provider was capable of removing encryption form the device of a terrorism suspect without weakening other devices in the market then the provider could be compelled under a technical assistance notice to provide help to the agency by removing the electronic protection. The mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built. The nature and scope of any weakness and vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required.[110]

The AHRC considered that more clearly defining the meaning of 'systemic vulnerability' and 'systemic weakness' in the Bill would enhance the efficacy of the safeguard, as well as providing greater certainty about the extent to which the Bill may impinge on the rights of users of technology.[111]

Similarly, the Communications Alliance, AI Group, AIIIA and AMTA submission stated:

> Unfortunately, neither the term systemic weakness/vulnerability, nor the term electronic protection has been defined in the draft Bill. It is unclear at what point a requested weakness would become systemic, i.e. would a weakness be systemic when a certain system is involved or does the concept of systemic revolve around the number of users (potential or actual?) affected by the weakness and, if so, what would a relevant user number threshold be? It is also not clear how vendors of telecommunications network equipment could be required to do a SAT [specified act or thing] without introducing a systemic weakness or vulnerability given that their products are at the core of most digital communications. Similarly, it is not clear what a weakness or vulnerability would be in the eyes of the requesting agency.[112]

The Digital Industry Group Inc (which included representatives from Amazon, Facebook, Google, Oath, and Twitter) highlighted practical issues with the new powers in the Bill. These included that while a provider cannot be required to implement or build a systemic weakness or a systemic vulnerability into a form of electronic protection, it can still be required to implement or build systemic weaknesses or vulnerabilities into any other component of a network, system, product or service. It regarded the Bill as 'fundamentally flawed':

> Deliberately creating a means of access to otherwise secure data will create weaknesses and vulnerabilities that, regardless of the good intentions at the time, will give an opportunity for other actors – including malicious ones – to access that same data, as well as having a host of other unintended consequences. It will reduce the security and privacy that Australians, Australian business, and the Australian economy rely upon every single day. Put simply, if you create a vulnerability in a technology that allows access to otherwise secure data then that vulnerability is capable of being exploited by any other party with the knowledge and means to do so.[113]

---

110. Explanatory Memorandum, pp. 67–68.
111. AHRC, Submission to DoHA, op. cit., p. 29.
112. Communications Alliance, AI Group, AIIA and AMTA, Submission to PJCIS, op. cit., p. 15.
113. Digital Industry Group Inc (DIGI), Submission to PJCIS, [Supplementary Submission 78.1], 27 November 2018, p. 1.

Issue: 'reasonable and practicable' requirements and when compliance is 'practicable and technically feasible'

The Attorney-General must not give a TCN to a designated communications provider unless the Attorney-General is satisfied that the requirements are reasonable and proportionate, and that compliance with the notice is practicable and technically feasible (**proposed section 317V)**. The same requirements apply to TANs (**proposed section 317P**). There is a need for greater specificity and definition of these terms.

While the Communication Alliance, AI Group, AIIA and AMTA submission was pleased that sections had been added to the Bill to provide guidance as to what requirements are 'reasonable and practicable' (**proposed sections 317RA** and **317ZAA**), it highlighted the lack of guidance as to when compliance is 'practicable' and 'technically feasible'. It proposed a guidance list including:

- a requirement to also consider the assessment of reasonableness, proportionality, technical feasibility and practicality as provided by the respective communications provider
- a clear principle that a specified act or thing be requested at the level in the supply chain that is least onerous for the communications provider involved, and more importantly, with a view to minimising additional cybersecurity risks or intrusion into privacy rights
- providing for compensation if a designated communications provider carries out the requested act or thing, and the execution of that act or thing causes damage and
- details on the timeframe for the assessment of technical feasibility as an act or thing may be considered technically feasible but only in a very extended timeframe.[114]

Issue: ambiguities in the various decision-making thresholds, conditions, limitations and procedural provisions

In her detailed submission, the IGIS identified some technical difficulties with parts of **Schedule 1** which could be addressed by the Parliament. **Proposed section 317ZH** will outline some general limitations on TANs and TCNs by providing that the notice has no effect to the extent (if any) that it would require a designated communications provider to do an act or thing for which a warrant or authorisation is required under a law of the Commonwealth, a state or territory, including the *TIA Act*, the *SD Act,* the *Crimes Act,* the *ASIO Act*, or the *Intelligence Services Act 2001*. The IGIS noted that the reference to the *Intelligence Services Act* in **proposed paragraph 317ZH(1)(e)** needs to be explained, because the agencies that are subject to the ministerial authorisation requirements in the *Intelligence Services Act* have no ability to issue TANS or request that the Attorney-General issues a TCN.[115]

Issue: significant change to the existing statutory immunities from legal liability on intelligence agencies

The IGIS noted that the existing arrangements relevant to ASIO are found in the special intelligence operations (SIO) scheme under Division 4 of Part III of the *ASIO Act* where there are significantly more safeguards than those in **proposed Part 15** of the *Telecommunications Act*:[116]

> These include requirements for Ministerial-level approval; proportionality and other requirements in the issuing criteria that limit the conduct able to be authorised; exclusions of certain acts from the immunity; and reporting and notification requirements to IGIS and the Attorney-General.[117]

---

114. Communications Alliance, AI Group, AIIA and AMTA, Submission to PJCIS, op. cit., pp. 14–15.
115. IGIS, Submission to PJCIS, op. cit., p. 14.
116. Ibid., p. 6.

Further:

> The current immunities from legal liability relevant to ASD and ASIS are in section 14 of the *Intelligence Services Act 2001* (ISA) and section 476.5 of the [Criminal] *Code*… One effect of the amendments in Schedule 1 is that intelligence agencies will potentially have multiple grounds of statutory immunity from civil and criminal liability that they could apply to communications providers who perform functions for them, which apply different thresholds and are subject to different conditions and limitations.[118]

Issue: offences relating to unlawful disclosure

The new unauthorised disclosure provisions carry a maximum penalty of imprisonment for five years (**proposed section 317ZF)**. The extensive provisions cover disclosures in a wide range of circumstances by a designated communications provider, entrusted ASIO, ASIS or ASD person, and others. The AHRC noted that specified persons could commit an offence if they disclose the 'very existence or non-existence of a request or notice, and the 'acts or things' done in compliance'.[119]

There are general exceptions to disclosure offence provisions, including in the context of legal proceedings or reports of such proceedings and in connection with the performance or the exercise of powers by the intelligence and interception agencies. The Explanatory Memorandum states that the exceptions in **proposed subsection 317ZF(3)** 'allow for the smooth administration of the Part and for the efficient exchange of information within law enforcement, security and intelligence agencies that seek or require assistance from providers'.[120]

The AHRC expressed significant concerns that the provisions are disproportionate, an unnecessary limit on freedom of expression, and 'potentially limit the right of citizens to take part in the conduct of public affairs, under Article 25 of the ICCPR.'[121] It stated:

> The Commission considers that it has not been demonstrated that all request or notice information, or information obtained under a request or notice, is of sufficient importance to justify secrecy, let alone criminal sanctions for disclosure. It is particularly difficult to justify criminalising disclosures that do not negatively affect national security or public safety, and where there has been no harm to the essential public interest.
>
> There may be further instances where the public interest in disclosure of certain information is warranted, where the essential public interest is not harmed. For example, it is not clear that it is appropriate to keep government contracting arrangements with providers in relation to 'acts or things' under TARs, wholly subject to secrecy.[122]

The justification provided in the Explanatory Memorandum is that the offences are necessary because 'there is a high risk that the release of sensitive information contrary to this subsection will cause significant harm to essential public interests, including national security and protection of public safety'.[123]

---

117. Ibid., pp. 6–7.
118. Ibid., p. 7.
119. AHRC, Submission to PJCIS, op. cit., p. 48.
120. Explanatory Memorandum, p. 66.
121. AHRC, Submission to PJCIS, op. cit., p. 48.
122. Ibid., p. 50.
123. Explanatory Memorandum, p. 65.

Privacy, data protection and cyber issues

During consultation on the Exposure Draft, the LCA noted that while there is 'significant value to public safety' in facilitating access to encrypted information, the 'protection of privacy should continue to be a fundamental consideration in and the starting point for any legislation providing access to telecommunications for security and law enforcement purposes'.[124]

The Government has emphasised that the assistance that agencies may request or compel from providers is not arbitrary, as it is prescribed by law. Further:

> … the Bill will assist agencies to fulfil their functions in a digital environment characterised by encryption and enable them to discharge their law enforcement and security functions more effectively. Terrorism, espionage, acts of foreign interference and serious and organised crime are regularly conducted through electronic communication services and devices operated by private providers. Industry is in a unique position to help agencies degrade, disrupt and prosecute criminal activity of this kind.[125]

However, several internet and technology providers expressed concern that the 'draft legislation bears the very real risk of severely damaging domestic and international cybersecurity and, therefore to act contrary to its stated aims'.[126] For example, Digital Industry Group Inc stated:

> Consumers will be rightly concerned that intervention by government agencies to create weaknesses and vulnerabilities in technology products and services will put the privacy and security of data, including their communications, purchases, images, videos, interactions and online activities, at risk. We believe that this loss of trust may dampen adoption and use of digital technology in Australia, and the use of Australian technology abroad, potentially reversing economic gains and social connectivity from which Australians have benefited.[127]

Compliance and Enforcement—Division 5

Issue: significant penalties for failure to comply with notices

A carrier or carriage service provider must comply with the notice requirements to the extent that the carrier or provider is capable of doing so (**proposed subsection 317ZA(1)**). Further, a person will be subject to a civil penalty if there is interference that leads to a carrier not complying with the notice requirements. Explicitly, a person must not:

- aid, abet, counsel or procure a contravention of subsection 317ZA(1)
- induce, whether by threats or promises or otherwise, a contravention of subsection (1)
- be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1) or
- conspire with others to effect a contravention of subsection (1).

Other designated communications providers (that are not carriers or carriage service providers) are also required to comply with a requirement under a TAN or TCN, to the extent that they are capable of doing so (**proposed section 317ZB**).

The penalty provisions in **Schedule 1** that have attracted some attention by stakeholders are the penalties for designated communications providers failing to comply with the requirements of a

---

124. LCA, Submission to DoHA, *Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, 10 September 2018, p. 20.
125. Explanatory Memorandum, p. 11.
126. Communications Alliance, AIIA and AMTA, Submission to DoHA, op. cit., p. 13.
127. Digital Industry Group, Supplementary Submission to PJCIS, op. cit., p. 6.

TAN or a TCN.[128] The penalties for carriers and carriage service providers, as opposed to other designated communications providers, are differentiated in the Bill.

A failure by a carrier or carriage service provider to comply with TAN or TCN requirements will attract the pecuniary penalties set out at Part 31 of the *Telecommunications Act*. That Part provides a maximum penalty of $250,000 for a body corporate and $50,000 for others.[129]

A failure by a designated communications provider (other than a carrier or carriage service provider) to comply with TAN or TCN requirements will attract a maximum penalty of 47,619 penalty units (currently $9,999,990) if it is a body corporate; for other providers it will be 238 penalty units (currently $49,980) (**proposed section 317ZB**).[130] This provision will be enforceable under Part 4 (civil penalty provisions); Part 6 (enforceable undertakings) and Part 7 (injunctions) of the *Regulatory Powers (Standard Provisions) Act 2014* (**proposed sections 317ZC** to **317ZE**).

Issue: conflict of laws

The DIGI submission noted that the Bill 'makes explicit its intended reach beyond the borders of Australia to any technology provider with a connection to Australia'. It considered that this 'causes major problems for businesses and it could ultimately put Australians at risk':

> A Notice may compel businesses with operations or customers outside Australia to take actions in Australia that violate the laws of other countries in which they operate. When those laws conflict, the businesses would be left having to arbitrate between them or decide whose laws to violate, knowing that in doing so they might risk sanctions. The Bill does include a defense to noncompliance with a Notice if it requires an action in a foreign country that would contravene the laws of that country, but there is no defense if a Notice requires a recipient to do an act or thing in Australia that might violate the laws of another country in which it operates or has customers.[131]

Computer access warrants: key issues and provisions in Schedule 2

Schedule 2 of the Bill will:

- expand the powers available under computer access warrants and authorisations executed by ASIO
- introduce computer access warrants for law enforcement agencies under the *SD Act*
- make related amendments to the *Mutual Assistance in Criminal Matters Act* and the *TIA Act* and
- amend the *TIA Act* to allow carriers to assist security authorities in activities relating to developing or testing technologies or interception capabilities.

ASIO computer access warrants and authorisations

Background

The *ASIO Act* was amended in 1999 to allow ASIO to apply for computer access (CA) warrants, with the regime expanded in 2014 to take account of technological developments.[132] The 2014 amendments included expanding the definitions of ***computer*** and ***target computer***, allowing third

128. See for example AHRC, Submission to PJCIS, op. cit., p. 33.
129. Section 570 of the *Telecommunications Act*.
130. *Crimes Act*, section 4AA (value of a penalty unit).
131. Digital Industry Group (DIGI), Supplementary Submission to PJCIS, op. cit., p. 12.
132. *Australian Security Intelligence Organisation Legislation Amendment Act 1999*, Schedule 1; *National Security Legislation Amendment Act (No. 1) 2014*, Schedule 2.

party computers and ***communications in transit*** to be used to access data in target computers, and allowing disruption of third party computers in certain circumstances for the purposes of executing a computer access warrant.[133]

The Attorney-General may issue a CA warrant under section 25A of the *ASIO Act* if he or she is satisfied that there are reasonable grounds to believe that access by ASIO to data held in a ***target computer*** will substantially assist the collection of intelligence about a matter that is important in relation to ***security***.[134] Under such a warrant, ASIO may be permitted to take certain actions for the purpose of accessing the relevant data, including entering premises, operating equipment and, in certain circumstances, using a communication in transit. ASIO may also do anything reasonably necessary to conceal those actions, which are undertaken covertly.[135]

Warrants issued under section 27A of the *ASIO Act* in relation to ASIO's function of obtaining foreign intelligence within Australia may authorise ASIO to do specified things that would be permitted under a computer access warrant that the Attorney-General considers appropriate in the circumstances. The Attorney-General may issue such a warrant if satisfied on the basis of advice from the Minister for Defence or Foreign Affairs that the collection of foreign intelligence relating to a specified matter is in the interests of Australia's national security, its national economic well-being or its foreign relations.

ASIO may also obtain an authority for computer access under an ***identified person warrant*** (IP warrant). These warrants are authorised by the Attorney-General and provide conditional approval for ASIO to exercise one or more specified powers in relation to a person if the Attorney-General is satisfied of certain matters.[136] If such a warrant has been issued and gives conditional approval for ASIO to access computer data, the Attorney-General or the Director-General of Security may give an authority to do certain things in relation to a computer if he or she is satisfied on reasonable grounds that doing specified things will substantially assist the collection of intelligence relevant to the ***prejudicial activities*** of the identified person.[137]

Overview of amendments

The amendments to the *ASIO Act* in **Schedule 2** of the Bill will add two further actions to those that ASIO may be permitted to take under a CA warrant, a foreign intelligence warrant or an authority for computer access under an IP warrant, namely:

- intercepting a communication passing over a telecommunications system for the purposes of doing something specified in the warrant or authority and
- removing a computer or other thing from premises for the purposes of doing something specified in the warrant or authority (and returning it afterwards).[138]

---

133. *National Security Legislation Amendment Act (No. 1) 2014*; item 4 of Schedule 2 (definition of ***computer***), items 18 and 41 (definitions of ***target computer***), items 23 and 25 (use of third party computers and communications in transit and disruption of third party computers). See further M Biddington and C Barker, *National Security Legislation Amendment Bill (No. 1) 2014*, Bills digest, 19, 2014–15, Parliamentary Library, Canberra, 28 August 2014, pp. 12–15; PJCIS, *Advisory report on the National Security Legislation Amendment Bill (No. 1) 2014*, PJCIS, Canberra, September 2014.
134. *Australian Security Intelligence Organisation Act 1979* (*ASIO Act*), subsections 25A(1) and (2). ***Security*** is defined in section 4 of the *ASIO Act*.
135. Ibid., subsections 25A(4) and (5).
136. Ibid., section 27C.
137. Ibid., section 27E. Under section 22, '***prejudicial activities*** of a person means activities prejudicial to security that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in'.
138. **Items 5** and **6** of **Schedule 2**, amending subsection 25A(4) of the *ASIO Act* (computer access warrants) and **items 10** and **11** of **Schedule 2**, amending subsection 27E(2) (authority for computer access under an identified person warrant). Subsection 27A(1) allows for things that would be permitted under subsection 25A(4) to be permitted under a foreign intelligence warrant issued under section 27A.

The amendments will also allow ASIO to take measures (including telecommunications interception) to conceal things done under a CA warrant, foreign intelligence warrant for computer access, or authority for computer access under an IP warrant:

- while the warrant or authority is in force and
- within 28 days following expiry of that warrant or authority, or the earliest opportunity thereafter.[139]

The current general prohibition on interception under a CA warrant or authorisation will also be removed, and will not be replaced by a prohibition on doing anything that would require a warrant under the *TIA Act*.[140]

Interception of communications

Under the *ASIO Act*, as it currently stands and as amended by the Bill, ***intercept a communication passing over a telecommunications system*** takes the same meaning as in the *TIA Act*, under which it consists of 'listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication'.[141]

The Explanatory Memorandum states that it is 'almost always necessary for ASIO to undertake limited interception for the purposes of executing a computer access warrant'.[142] It does not state why this is the case. Of likely relevance, under subsection 25A(4) of the *ASIO Act*, among the things that the Attorney-General may permit ASIO to do under a CA warrant are:

- using a telecommunications facility for the purpose of obtaining access to data relevant to the security matter for which the warrant was issued (***relevant data***) that is held in the target computer at any time the warrant is in force
- using a communication in transit to access ***relevant data*** and if necessary, adding, copying, deleting or altering other data in that communication (if, having regard to other methods, if any, of obtaining access to the relevant data that are likely to be as effective, it is reasonable to do so) and
- copying any data to which access has been obtained that appears to be relevant to the collection of intelligence by ASIO in accordance with the *ASIO Act* (not just ***relevant data***).[143]

However, if doing any of those things, or anything else permitted under a CA warrant, would constitute ***intercepting a communication passing over a telecommunications system***, ASIO must currently obtain a separate telecommunications interception warrant under the *TIA Act* before taking such action.[144]

Item 6 of **Schedule 2**, in conjunction with **item 13**, will amend the *ASIO Act* so that under a CA warrant or a foreign intelligence warrant, the Attorney-General could instead permit ASIO to ***intercept a communication passing over a telecommunications system*** 'if the interception is for

---

139. **Item 7** of **Schedule 2**, inserting **proposed subsection 25A(8)** of the *ASIO Act* (computer access warrants); **item 8**, inserting **proposed subsection 27A(3C)** (warrants for the purpose of obtaining foreign intelligence within Australia); **item 12**, inserting **proposed subsection 27E(6)** of the *ASIO Act* (authority for computer access under an identified person warrant).
140. See subsection 33(1) of the *ASIO Act* and **item 13** of **Schedule 2** to the Bill.
141. *ASIO Act*, subsections 33(1) and (2); **item 1** of **Schedule 2** to the Bill; *TIA Act*, subsection 6(1).
142. Explanatory Memorandum, p. 80.
143. The same things may also permitted under a foreign intelligence warrant (see subsection 27A(1) of the *ASIO Act*) and a computer access authority issued under an IP warrant (see subsection 27E(2)). There are limitations on adding, deleting and altering data in subsections 25A(5) and 27E(5).
144. *ASIO Act*, subsection 33(1).

the purposes of doing any thing specified' in that warrant if he or she considers it appropriate in the circumstances (on **item 13**, see further below under the issue heading).[145]

Item 11 of **Schedule 2**, in conjunction with **item 13**, will make an equivalent amendment in relation to computer access authorities given under IP warrants.

The Explanatory Memorandum advances two arguments in support of the proposed change, namely that:

- the different thresholds that apply to the issue of CA warrants under the *ASIO Act* and interception warrants under the *TIA Act* mean that ASIO is sometimes able to obtain a CA warrant but not the interception warrant it would require to execute the CA warrant and
- it is administratively inefficient to require ASIO to apply for, and the Attorney-General to consider, two different warrants with different legal thresholds, for the purposes of executing a CA warrant.[146]

Authorising telecommunications interception outside of the framework provided under the *TIA Act*, and based upon a lower threshold than applies under the *TIA Act*, is a significant change. The Scrutiny of Bills Committee, PJCHR and some stakeholders questioned whether the challenges highlighted above are sufficient justification for the proposed change.[147] While interception is only intended to be permitted for the purpose of executing a CA warrant (not collecting intelligence), the new power has been cast quite broadly. Parliamentarians may wish to consider amendments to ensure that interception is authorised under a CA warrant only to the extent necessary to execute the warrant, and is accompanied by appropriate safeguards and oversight.

Issue: no prohibition on interception that would require a TIA Act warrant

Item 13 will repeal subsection 33(1) of the *ASIO Act,* which provides that nothing in section 25A (CA warrants), 27A (foreign intelligence warrants) or 27E (computer access authorities under IP warrants), or in warrants or authorities issued under those sections, authorises ASIO to intercept a communication passing over a telecommunications system operated by a carrier or a carriage service provider. Consideration should be given to replacing subsection 33(1) with a provision to the effect that nothing in the *ASIO Act* authorises the doing of anything for which a warrant would be required under the *TIA Act*.[148] This would make clearer the intended limits on interception under CA warrants and provide certainty that CA warrants cannot be used to undertake interception for the purposes of collecting intelligence.

Issue: breadth of interception powers under a CA warrant

CA warrants authorise ASIO to do specified things that the Attorney-General considers appropriate in the circumstances. The Bill will add interception (for the purposes of doing anything else specified in the warrant) to the list of things that may be specified.

Unlike warrants issued under the *TIA Act*, the Bill will not require the CA warrant to identify a particular telecommunications service or person in relation to which interception is authorised.[149] The IGIS noted that this may reflect an intent that the key statutory limitation on interception under a CA warrant is the purpose for which it is undertaken, but stated:

---

145. **Item 6** will insert **proposed paragraph 25A(4)(ba)** into the *ASIO Act*. Subsection 27A(1) of the *ASIO Act* allows for things that would be permitted under subsection 25A(4) to be permitted under a foreign intelligence warrant issued under section 27A.
146. Explanatory Memorandum, p. 80.
147. Scrutiny of Bills Committee, *Scrutiny digest*, op. cit., pp. 30–32; PJCHR, *Human rights scrutiny report*, op. cit., pp. 58–61; LCA, Submission to PJCIS, op. cit., pp. 35–37; AHRC, Submission to PJCIS, op. cit., pp. 68–72.
148. See for example subsection 18(7) and 32(4) of the *Surveillance Devices Act 2004* (*SD Act*).
149. *TIA Act*, sections 9 and 9A (issue of telecommunications service and named person warrants) and 11A and 11B (equivalent warrants for collection of foreign intelligence).

> Nonetheless, the absence of a requirement to specify telecommunications services or persons will further expand the powers available to ASIO under its computer access warrants. These powers are already broad, including as a result of the definition of a 'computer', the 'security matter' or 'foreign intelligence matter' in respect of which warrants can be issued, and the applicable issuing thresholds.
>
> Even taking into account the anticipatory nature of intelligence collection activities under ASIO's special powers warrants, the result is that the exercise of TI powers might be authorised on a much broader scale than may be immediately apparent on the face of the provisions, and on a broader scale than would be permitted under the *TIA Act*.[150]

The Bill will allow a CA warrant to authorise interception for the purposes of doing 'any thing specified in the warrant'. However, not all of the things that may be specified in a CA warrant relate to accessing relevant data. For instance, a warrant may authorise entering premises for the purposes of executing a CA warrant.[151] The IGIS, LCA and AHRC recommended that interception instead be authorised only for things that may be authorised under a CA warrant that concern accessing relevant data.[152] It may be appropriate to allow interception to be authorised also for the purpose of doing anything reasonably necessary to conceal the fact that something has been done under a CA warrant.[153]

A CA warrant may only authorise ASIO to use another computer or a communication in transit to obtain access to relevant data 'if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so'.[154] Consideration could be given to an equivalent limitation on the authorisation of interception under a CA warrant.

A CA warrant must authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant.[155] Interception warrants issued under the *TIA Act* do not authorise the use of force. While the IGIS questioned whether use of force could ever be necessary or reasonable to intercept a communication under a warrant, it may be more appropriate to amend the provisions relating to use of force to exclude interception from their application.[156] In a supplementary submission to the PJCIS, DoHA noted that some submissions suggested that use of force not be permitted for the purposes of interception and argued:

> … it is long standing practice that entry onto premises may be necessary where it would be impractical or inappropriate to intercept communications in respect of a device otherwise than by using equipment installed on specified premises. This may be due to technical reasons connected with the operation of the service or the telecommunications system of which the service is part, or because the execution of the computer access warrant as a result of action taken by an officer of a carrier might jeopardise the security of the investigation. Accordingly, it is reasonable and necessary to ensure that law enforcement

150. Footnote references have been omitted from this quotation and can be viewed in the source document: IGIS, Submission to PJCIS, op. cit., pp. 40–41. See also LCA, Submission to PJCIS, op. cit., pp. 35–37.
151. *ASIO Act*, subsection 25A(4). See also subsection 27E(2).
152. IGIS, Submission to PJCIS, op. cit., p. 41; LCA, Submission to PJCIS, op. cit., p. 39; AHRC, Submission to PJCIS, op. cit., pp. 70–72. This could be achieved by limiting interception to the purposes of doing things set out in paragraphs 25A(4)(a) and (ab) and 27E(2)(c) and (d) of the *ASIO Act*.
153. This may be permitted under paragraphs 25A(4)(c) and 27E(2)(f).
154. *ASIO Act*, paragraphs 25A(4)(ab) and 27E(2)(d).
155. *ASIO Act*, paragraphs 25A(5A)(a), 27A(2)(a) (foreign intelligence warrants) and 27J(3)(d) (authorities under IP warrants).
156. The LCA and AHRC recommended such amendments; the IGIS recommended such an amendment if the intent is not to authorise the use of force: LCA, Submission to PJCIS, op. cit., p. 39; AHRC, Submission to PJCIS, op. cit., pp. 72–73; IGIS, Submission to PJCIS, op. cit., pp. 42–43.

officers undertaking these activities can do so with appropriate authorisations around the use of force.[157]

Issue: accountability and oversight

Section 34 of the *ASIO Act* requires ASIO to submit reports to the Attorney-General on the extent to which actions taken under each warrant assisted the agency in carrying out its functions. The Bill does not include an amendment to require that such reports include, for CAs, details of any interception activities undertaken. As the IGIS pointed out, this would mean that interception under a CA warrant would be subject to less detailed reporting than interception under the *TIA Act*. The IGIS recommended that reports under section 34 for CA warrants should be required to address the same matters as reports under section 17 of the *TIA Act* in relation to interception activities (the extent to which the interception assisted the agency in carrying out its functions and the telecommunications service to or from which each intercepted communication was made).[158]

Removing things from premises

As noted above, CA warrants authorise ASIO to do specified things that the Attorney-General considers appropriate in the circumstances. **Item 5** of **Schedule 1** will expand the list of things that may be specified under a CA warrant (or a foreign intelligence warrant that authorises computer access) to include removing a computer or other thing from premises temporarily for the purpose of doing any thing specified in the warrant.[159] **Item 10** will make an equivalent amendment in relation to computer access authorities given under IP warrants.

Issue: breadth of the new power

As with the proposed interception power, temporary removals will be authorised for the purposes of doing 'any thing specified in the warrant'. Again, it may be more appropriate to limit authorisation for removal of things to doing only some of the things that may be specified under a CA warrant. The most relevant would be those relating to accessing relevant data, copying data that appears relevant, and doing anything reasonably necessary to conceal the fact that something has been done under a CA warrant.[160]

As the IGIS and the LCA pointed out, the Bill will not put any limit on what sort of objects could be removed from premises as 'other things'.[161] If the purpose of removing things is to obtain access to data, it may be more appropriate to limit the removals power to computers, data storage devices, and possibly other electronic equipment.

Finally, ASIO would be permitted to remove computers and other things from 'premises'. This would include both premises specified in the warrant and other premises entered for the purpose of gaining entry to or exit from the specified premises. Consideration could be given to limiting the removals power to 'specified premises'.

---

157. DoHA, Supplementary submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 18.3], n.d., p. 6.
158. IGIS, Submission to PJCIS, op. cit., p. 43.
159. **Proposed paragraph 25A(4)(ac)**. Subsection 27A(1) of the *ASIO Act* allows for things that would be permitted under subsection 25A(4) to be permitted under a foreign intelligence warrant issued under section 27A.
160. Under paragraphs 25A(4)(a), (ab), (b) and (c) and 27E(2)(c), (d), (e) and (f). On this point, see: IGIS, Submission to PJCIS, op. cit., pp. 43–44; LCA, Submission to PJCIS, op. cit., p. 41.
161. IGIS, Submission to PJCIS, op. cit., pp. 43–44; LCA, Submission to PJCIS, op. cit., p. 41.

Issue: no time limit for return of things

As the IGIS and the LCA point out, the Bill will not specify a maximum time for which computers and other things may be removed from premises or include a requirement that things must be returned as soon as reasonably practicable.[162] The Explanatory Memorandum states that the removal 'is only permitted for the purposes of doing anything specified in the computer access warrant before the computer or other thing must be returned to the premises'.[163] While this may be the intent, it might be preferable for this limit to be explicit on the face of the provision, as it is in relation to things removed from premises for inspection under a search warrant or IP warrant.[164] A limitation of this type would still allow a record or other thing to be retained by ASIO where returning it would be prejudicial to security.

Issue: accountability and oversight

As noted above, section 34 of the *ASIO Act* requires ASIO to submit reports to the Attorney-General on the extent to which actions taken under each warrant assisted the agency in carrying out its functions. There will be no requirement for ASIO to include in such reports details about each time a computer or other thing is removed from premises under a CA warrant. The IGIS considered that the absence of such a reporting requirement 'may also mean that suitably detailed records may not be made (or may not be made consistently) of the reasons for, and duration of, each removal', impeding effective oversight.[165] The IGIS suggested such a reporting requirement be included, and noted that this would also help it to monitor ASIO's compliance with existing limits on material interference that will also apply where things are removed from premises.[166]

Concealment activities

ASIO may currently only do things to conceal the fact that something has been done under a CA warrant if the warrant provides specific authority to do so, and while the warrant is in force (the same is true for foreign intelligence warrants for computer access and authorities for computer access under an IP warrant).[167]

Item 7 of **Schedule 2** will insert **proposed subsection 25A(8**) into the *ASIO Act*. If any thing is done in relation to a computer under a CA warrant or under the proposed subsection, ASIO will be permitted to do certain things in order to conceal that fact while the warrant is in force or within 28 days afterwards. If no concealment action is taken within that 28 day period, ASIO will be permitted to do those things 'at the earliest time after that 28-day period at which it is reasonably practicable' to do so. **Items 8** and **12** will insert **proposed subsections 27A(3C)** and **27E(6)** to make equivalent provision for concealing things done under foreign intelligence warrants for computer access, authorities for computer access under an IP warrant, and the proposed subsections. These provisions mirror existing provisions allowing ASIO to recover surveillance devices after the expiry of a warrant or authority.[168]

---

162. IGIS, Submission to PJCIS, op. cit., pp. 44–45; LCA, Submission to PJCIS, op. cit., p. 41.
163. Explanatory Memorandum, p. 79.
164. *ASIO Act*, subsections 25(4C) and 27D(5). Consideration could be given to a similar limitation on the power to temporarily remove objects from premises for the purpose of installing or maintaining a surveillance device or enhancement equipment under paragraph 26B(4)(b) of the *ASIO Act*.
165. IGIS, Submission to PJCIS, op. cit., p. 45.
166. Ibid., pp. 45–46.
167. Ibid., subsections 25A(4) and 27E(2). Subsection 27A(1) of the *ASIO Act* allows for things that would be permitted under subsection 25A(4) to be permitted under a foreign intelligence warrant issued under section 27A.
168. *ASIO Act*, subsections 26B(5), 27A(3A), 27F(5) and (6).

The permitted concealment actions mirror the things that may be done in order to execute the warrant or authority, as amended by the Bill.

Issue: authorisation for concealment

ASIO may currently only undertake concealment activities if the Attorney-General considers it appropriate in the circumstances and authorises those activities in the relevant warrant. The Bill will permit concealment activities both while a warrant is in force and afterwards, without any specific authorisation. Consideration could be given to combining the existing and proposed provisions to remove this inconsistency. Concealment activities could remain something only permitted if specified in the warrant (having been determined to be appropriate in the circumstances), but able to be undertaken within a certain period after the warrant expires, and with the types of activities authorised set out in the Act.

Issue: no limit on material interference/causing material loss or damage

The *ASIO Act* provides that certain acts (including causing a material loss or damage to persons lawfully using computers) are not authorised in the course of doing things specified in a CA warrant.[169] However, as noted by some stakeholders, the Bill does not extend those limitations to things done under the proposed new concealment powers.[170] It would seem appropriate that the same limitations be applied to acts done under **proposed subsections 25A(8)** and **27E(6)**. In a supplementary submission to the PJCIS, DoHA indicated that the protections in subsections 25A(5) and 27E(5) have deliberately not been extended to cover concealment activities, but provided little justification for that position, stating: 'To maintain operational integrity it may be necessary to conceal activities through manipulation of data and while the safeguards don't apply here, the purposes for which they are abrogated are very limited'.[171]

Issue: concealment activities after the expiry of a warrant

The LCA was opposed to allowing concealments activities to be undertaken more than 28 days after expiry of a warrant.[172] The scrutiny committees and the AHRC suggested that concealment activities only be permitted more than 28 days after expiry of a warrant under a separate authorisation.[173]

Allowing ASIO to do things as soon as reasonably practicable after the 28 day period has passed is intended to enable ASIO to take concealment action later if it *could not* have done so within the 28 days.[174] If it is to be retained, the proposed provision might be improved by expressly limiting the authority to undertake concealment activities in such a way, instead of applying where those things *were not* done earlier (but possibly could have been).[175]

---

169. *ASIO Act*, subsections 25A(5) and 27E(5).
170. IGIS, Submission to PJCIS, op. cit., pp. 48–49; LCA, Submission to PJCIS, op. cit., p. 43; AHRC, Submission to PJCIS, op. cit., pp. 66–67.
171. DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 11.
172. LCA, Submission to PJCIS, op. cit., pp. 43–44.
173. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., pp. 34–35; PJCHR, *Human rights scrutiny report*, op. cit., pp. 53–54; AHRC, Submission to PJCIS, op. cit., p. 65–66. The Commonwealth Ombudsman raised a similar point in relation to CA warrants under the *SD Act*: Commonwealth Ombudsman, Submission to PJCIS, op. cit., p. 6. If a separate authorisation was introduced for ASIO to undertake concealment activities more than 28 days after expiry of a warrant, it would be consistent to introduce an equivalent requirement in relation to retrieval of surveillance devices.
174. Explanatory Memorandum, p. 81.
175. The same amendment could be made to the existing provision related to surveillance devices (paragraph 26B(5)(m)).

Issue: accountability and oversight

As noted above, section 34 of the *ASIO Act* requires ASIO to submit reports to the Attorney-General on the extent to which actions taken under each warrant assisted the agency in carrying out its functions. **Item 16** of **Schedule 2** will amend section 34 to provide that for the purposes of that section, anything done under **proposed subsections 25A(8)**, **27A(3C)** or **27E(6)** is taken to have been done under a warrant issued under section 25A, 27A or 27E. The IGIS suggested that consideration be given to inclusion of a separate reporting requirement for concealment activities carried out more than 28 days after the expiry of a warrant so as not to delay warrant reporting.[176]

Law enforcement computer access warrants under the SD Act

Schedule 2 of the Bill will amend the *SD Act* to allow Commonwealth and state and territory law enforcement officers to apply for computer access (CA) warrants, similar to those available to ASIO (as amended by the Bill). The purposes for which these warrants will be available will be the same as those for which surveillance device warrants may be issued, as will the thresholds for issue of a warrant.[177] A warrant may be issued by an eligible Judge or a nominated member of the Administrative Appeals Tribunal (AAT) if that person is satisfied of certain matters.

Definition of computer and meaning of target computer and implications for proposed powers

Item 36 of **Schedule 2** of the Bill will replace the existing definition of computer in subsection 6(1) the *SD Act* with a much broader definition, identical to that in the *ASIO Act*. Instead of meaning (as it currently does in the *SD Act*) 'any electronic device for storing or processing information', ***computer*** would mean one or more computers, one or more computer systems, one or more computer networks or a combination thereof.[178] The Explanatory Memorandum also notes that devices for storing and processing information that 'would not colloquially be termed "computers"', such as security systems, internet protocol cameras and digital video recorders, are intended to be captured by the definition.[179]

CA warrants (and emergency authorisations for computer access) will authorise access to data held in, and the doing of certain things in relation to, a ***target computer***. This may be a particular computer, a computer at particular premises, and/or a computer 'associated with, used by or likely to be used by, a person (whose identity may or may not be known)'.[180]

The breadth of these definitions has implications for the breadth of the powers authorised under a CA warrant. At its limit, a CA warrant will be able (providing the relevant thresholds in **proposed sections 27A** and **27C** are met) to authorise access to multiple computer networks across multiple locations on the basis that they are associated with or likely to be used by a person whose identity is not known.

Other definitions

Items 35 and **37–46** will amend or insert definitions in subsection 6(1) of the *SD Act*. Of particular note:

---

176. IGIS, Submission to PJCIS, op. cit., p. 49.
177. *SD Act*, sections 14 and 16; **item 49** of **Schedule 2**, **proposed sections 27A** and **27C**.
178. **Item 36** of **Schedule 2**. As noted above, the definition in the *ASIO Act* was expanded in this way in 2014.
179. Explanatory Memorandum, p. 88.
180. **Item 49** of **Schedule 2** (**proposed subsection 27A(15)** and **proposed section 27E**), **item 50** (**proposed subsection 28(1B)**), **item 52** (**proposed subsection 29(1B)**), **item 54** (**proposed subsection 30(1B)**).

- ***data*** will include information in any form, and any program or part of a program (but 'program' will not be defined)
- ***data held in a computer*** will include data held in any removable ***data storage device*** for the time being held in a computer, and data held in a data storage device on a computer network of which the computer forms a part (the Explanatory Memorandum states that the definition 'envisages both internal network storage, such as back-up copy of data, and external storage, such as internet-based and cloud-based storage'[181])
- ***intercepting a communication passing over a telecommunications system*** will have the same meaning as in the *TIA Act*, under which it consists of 'listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication'.[182]

Purposes of CA warrants

The amendments to the *SD Act* will allow ***law enforcement officers*** to apply for CA warrants for the purposes of:

- obtaining evidence of a ***relevant offence***, or the location or identity of an offender
- obtaining evidence of an offence, or the location or identity of an offender, in a mutual assistance investigation
- assisting in the location and safe recovery of a child (where a recovery order is in force)
- determining whether a control order has been or is being complied with, or obtaining information relating to the controlee that is likely to substantially assist in protecting the public from a terrorist act or preventing the provision of support for or facilitation of a terrorist act or engagement in hostile activity overseas or
- (for ***federal law enforcement officers only***), obtaining evidence relating to the integrity, location or identity of a staff member of an agency subject to integrity testing (AFP, ACIC and DoHA).[183]

As noted above, these are the same purposes for which surveillance device warrants may be issued. The thresholds that apply in order for a law enforcement officer to apply for a CA warrant for each purpose are equivalent to those for surveillance devices.[184]

Under the *SD Act*, ***relevant offence*** includes some specific Commonwealth offences; any Commonwealth offence or state offence that has a federal aspect and carries a maximum penalty of at least three years imprisonment; offences carrying a maximum penalty of at least 12 months that are suspected in the context of an integrity operation; and offences prescribed in the regulations.[185] ***Law enforcement officer*** includes ***federal law enforcement officers*** (certain officers

---

181. Explanatory Memorandum, p. 89.
182. *TIA Act*, subsection 6(1).
183. **Item 49** of **Schedule 2**, **proposed section 27A** of the *Surveillance Devices Act 2004* (*SD Act*); **items 25** and **26** of **Schedule 2**, amending the *Mutual Assistance in Criminal Matters Act 1987*. The amendments to the *Mutual Assistance in Criminal Matters Act* will allow the Attorney-General to permit an ***eligible law enforcement officer*** to apply for a CA warrant under **proposed section 27A** of the *SD Act* if satisfied of certain matters, including that the foreign criminal matter involves an offence against a law in the relevant country that carries a maximum penalty of at least three years imprisonment. This penalty threshold is consistent with the definition of ***relevant offence*** in the *SD Act*.
Part 3 of **Schedule 2** will amend the *International Criminal Court Act 2002* and the *International War Crimes Tribunals Act 1995* to allow the Attorney-General to permit an ***eligible law enforcement officer*** to apply for a CA warrant under **proposed section 27A** of the *SD Act* if the International Criminal Court or an international war crimes tribunal has requested that the Attorney-General arrange for access to data held in a computer and the Attorney-General is satisfied of certain matters. It will also make amendments to the *SD Act* consequential to those amendments and the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.
184. Ibid., section 14; **item 49** of **Schedule 2**, **proposed section 27A** of the *SD Act*.
185. *SD Act*, subsection 6(1). No offences have been prescribed in the regulations.

in the AFP, ACIC and ACLEI) and certain officers in state and territory police forces and anti-corruption agencies.[186]

Issuing of CA warrants

A CA warrant may be issued by an eligible Judge or a nominated member of the AAT if that person is satisfied of certain matters, including:

- for a warrant relating to a control order, that an order is in force in relation to a person, and that access to data in the target computer to obtain information about the person would be likely to substantially assist in protecting the public from a terrorist act or preventing the provision of support for or facilitation of a terrorist act or engagement in hostile activity overseas
- for warrants for the other purposes outlined above, that there are reasonable grounds for the suspicion/s founding the application, and where relevant, that a certain authority or order is in place.[187]

In considering whether to issue a warrant, the eligible judge or nominated AAT member must consider particular matters, including the extent to which anyone's privacy is likely to be affected, and the existence of alternative means to obtain the evidence or information.[188]

Actions permitted under CA warrants and after expiry of warrants

The eligible judge or nominated AAT member must specify which actions are permitted under the CA warrant.[189] The actions that may be permitted under a CA warrant will be equivalent to those that may be permitted under an ASIO CA warrant (as amended by the Bill)—in summary:

- entering *specified premises* for the purpose of executing the warrant
- entering *any premises* for the purpose of gaining entry to or exit from specified premises
- using the ***target computer***, a telecommunications facility, any other electronic equipment or a data storage device in order to access data held in that computer at any time while the warrant is in force to determine whether it is covered by the warrant; and if necessary to do so, adding, copying, deleting or altering other data in the target computer
- if, having regard to other methods of obtaining access to the relevant data that are likely to be as effective, it is reasonable in all the circumstances to do so, using *any other computer* or a *communication in transit* to access the relevant data; and if necessary to do so, adding, copying, deleting or altering other data in that computer or communication
- removing a computer *or other thing* from (any) premises for the purposes of doing any thing specified in the warrant, and returning it afterwards
- copying any data accessed that appears to be relevant for the purpose of determining whether the relevant data is covered by the warrant
- intercepting a communication passing over a telecommunications system for the purpose of doing any thing specified in the warrant and
- any other thing reasonably incidental to the above things.[190]

---

186. Ibid., subsection 6(1) and section 6A.
187. **Item 49** of **Schedule 2**, **proposed subsection 27C(1)** of the *SD Act*.
188. **Item 49** of **Schedule 2**, **proposed subsection 27C(2)** of the *SD Act*. The matters that must be considered depend on the purpose for which the warrant is sought.
189. **Item 49** of **Schedule 2**, **proposed subsections 27E(1)** and **(2)** of the *SD Act*.
190. The only difference in what may be authorised compared to ASIO CA warrants is that all concealment activity will be automatically authorised under **proposed subsection 27E(7)** (equivalent to **proposed subsection 25A(8)** of the *ASIO Act*)

Like ASIO CA warrants, those for law enforcement officers will be executed covertly, and officers will be authorised to do things to conceal actions taken under such a warrant. Like ASIO, law enforcement officers will be permitted under proposed **subsection 27E(7)** to undertake concealment activities while the warrant is in force or within 28 days afterwards, and if no concealment action is taken within that 28 day period, will be permitted to do those things 'at the earliest time after that 28-day period at which it is reasonably practicable' to do so.[191]

Issues in relation to actions permitted under and after the expiry of CA warrants

Many of the issues outlined earlier in this Digest in relation to ASIO CA warrants, in particular the lack of a prohibition on interception that would require a *TIA Act* warrant (see page 34),[192] the breadth of the proposed interception powers (see pages 34–35), the breadth of the proposed object removal powers (see page 36), the lack of a time limit on the removal power (see page 36), and the issues raised in relation to concealment activities (see pages 37–38), also arise in relation to CA warrants for law enforcement officers.[193]

Other issues relating to CA warrants for law enforcement officers, and to the use of information obtained through interception under an ASIO CA warrant or a law enforcement CA warrant, are outlined below.

Issue: concealment activities after the expiry of a warrant

Allowing ASIO to undertake concealment activities after a CA warrant expires is consistent the agency's powers in relation to retrieval of surveillance devices. This is not the case for law enforcement officers. Under the *SD Act*, a law enforcement officer must apply for a separate retrieval warrant in order to retrieve a surveillance device (and conceal the fact that it has been retrieved) after the relevant warrant has expired.[194] The Explanatory Memorandum acknowledges this difference but argues against inclusion of a separate authorisation for concealment activities after expiry of a CA warrant on the basis of 'the importance of ensuring that agencies have the ability to determine when access to premises or to a planted device will best ensure the operation remains covert', stating that it 'will not always be possible to predict when safe retrieval of a device can be performed without compromising an investigation'.[195] However, it is not clear how those arguments apply to a greater degree to concealment related to computer access than to retrieval of a surveillance device. As noted above, the scrutiny committees and the AHRC suggested that concealment activities only be permitted more than 28 days after expiry of a warrant under a separate authorisation.[196]

---

instead of also being something that the issuer may authorise under **proposed subsection 27E(2)** (equivalent to subsection 25A(4) of the *ASIO Act*).

191. **Item 49** of **Schedule 2**, **proposed subsection 27E(7)** of the *SD Act*.
192. This prohibition would exist in relation to emergency authorisations (existing subsection 32(4) of the *SD Act*) but not for CA warrants.
193. See also: Scrutiny of Bills Committee, *Scrutiny digest*, op. cit., pp. 30–35, ; PJCHR, *Human rights scrutiny report*, op. cit., pp. 43–47, 49–50, 51–54, 58–61; AHRC, Submission to PJCIS, op. cit., pp. 58–73; LCA, Submission to PJCIS, op. cit., pp. 33–44; Commonwealth Ombudsman, Submission to PJCIS, op. cit., pp. 5–6.
In relation to concealment activities, the issue of authorisation of concealment activities will be somewhat different under the *SD Act* because concealment activities will be authorised solely automatically under **proposed subsection 27E(7)** of the *SD Act*; they will not also be able to be specified in the warrant as a permitted action under **proposed subsection 27E(2)**.
194. *SD Act*, Division 3 of Part 2.
195. Explanatory Memorandum, pp. 98–99 (quotes taken from p. 99).
196. Scrutiny of Bills Committee, *Scrutiny digest*, op. cit., pp. 34–35; PJCHR, *Human rights scrutiny report*, op. cit., pp. 53–54; AHRC, Submission to PJCIS, op. cit., p. 65–66. The Commonwealth Ombudsman suggested that extensions to CA warrants should be sought where an agency needs additional time for concealments actions (instead of such actions being permitted more than 28 days after expiry): Commonwealth Ombudsman, Submission to PJCIS, op. cit., p. 6. A separate authorisation similar to

Issue: potential impact on parliamentary privilege

The President of the Senate wrote to the PJCIS, the Attorney-General and the Minister for Home Affairs to raise concerns about the interaction of CA warrants under the *SD Act* and expanded search powers in the *Crimes Act* and *Customs Act* (included in **Schedules 3** and **4** of the Bill respectively) with parliamentary privilege.[197] He noted that the protection of parliamentary material from seizure under search warrant is dealt with in the memorandum of understanding between the Parliament and the Executive on the AFP's execution of search warrants, and that work is currently underway to develop a protocol for the exercise of other investigative powers:[198]

> A particular concern to the Senate committee in relation to the covert use of such powers was the question [of] how claims of parliamentary privilege can be raised and resolved when no-one with standing to make a claim is aware that such information is being accessed. These concerns may be exacerbated by the provisions of the Assistance and Access Bill 2018.[199]

The President of the Senate accepted that the Bill would not abrogate parliamentary privilege, but indicated that it would be important to reach agreement (either before or after passage of the Bill) on how potential claims of parliamentary privilege arising from the exercise of covert powers would be dealt with in practice. He considered that an effective solution would likely require a combination of procedural and legislative action.[200]

Duration of warrants

Warrants may be issued for a period of up to 90 days (or 21 days if issued for the purpose of an integrity operation) and could be extended by an eligible judge or nominated AAT member by up to 90 days (or 21 days) at a time.[201] These limits are the same as those for surveillance device warrants.[202]

CA warrants may be revoked earlier by an eligible judge or nominated AAT member.[203] The chief officer of the relevant law enforcement agency must apply for a warrant to be revoked if he or she is satisfied that access to data under the warrant is no longer required for the purpose for which the warrant was issued (or if the authority for the integrity operation or control order in relation to which the warrant was issued is no longer in force).[204] It is not clear why a revocation must not also be sought if the recovery order in relation to which the warrant was issued is no longer in force.[205]

Emergency authorisations for access to data held in a computer

Part 3 of the *SD Act* allows a law enforcement officer to apply to an ***appropriate authorising officer*** for an emergency authorisation for the use of a surveillance device in certain

---

retrieval warrants may be preferable, as the threshold for extending a warrant may not be met if sought only to conceal something done under a warrant.

197. Ryan, Submission to PJCIS, op. cit.
198. The Memorandum of understanding on the execution of search warrants in the premises of members of Parliament is reflected in the AFP National Guideline for execution of search warrants where parliamentary privilege may be involved.
199. Ryan, Submission to PJCIS, op. cit., pp. 1–2 (quote taken from p. 2).
200. Ibid., pp. 2–3.
201. **Item 49** of **Schedule 2**, **proposed subsection 27D(3)** and **proposed section 27F** of the *SD Act*.
202. *SD Act*, subsection 17(1A) and section 19.
203. **Item 49** of **Schedule 2**, **proposed subsection 27G(1)** of the *SD Act*.
204. **Item 49** of **Schedule 2**, **proposed subsection 27G(2)** and **proposed section 27H** of the *SD Act*.
205. This anomaly also exists for surveillance device warrants under sections 20 and 21.

circumstances. The heads of each ***law enforcement agency*** and certain senior officers within them are ***appropriate authorising officers***.[206]

Items 50–77 of **Schedule 2** of the Bill will amend Part 3 of the *SD Act* so that emergency authorisations may also be sought and made for access to ***data held in a computer***. The purposes for which emergency authorisations may be granted will be the same as for surveillance devices.[207] The purposes are fewer and narrower than those for which a CA warrant or surveillance device warrant may be issued.

A law enforcement officer may apply for an emergency authorisation for access to data held in a ***target computer*** if:

- in the course of an investigation of a ***relevant offence***, the officer reasonably suspects that:
  - an imminent risk of serious violence to a person or substantial damage to property exists
  - access to the data is immediately necessary for the purpose of dealing with that risk
  - the circumstances are so serious and the matter of such urgency that access is warranted and
  - it is not practicable in the circumstances to apply for a CA warrant or
- a recovery order is in force and the officer reasonably suspects that:
  - the circumstances are so urgent as to warrant immediate access to the data and
  - it is not practicable in the circumstances to apply for a CA warrant or
- the officer is conducting an investigation into one or more listed offences (including certain offences under the *Customs Act*, *Criminal Code* and the *Migration Act 1958*) and reasonably suspects that:
  - access to the data is immediately necessary to prevent the loss of any evidence relevant to that investigation
  - the circumstances are so serious and the matter of such urgency that access is warranted and
  - it is not practicable in the circumstances to apply for a CA warrant.[208]

An appropriate authorising officer may grant an application if satisfied of certain matters, including that there are reasonable grounds for the suspicion founding the application.[209]

Proposed subsection 32(2A) will provide that an emergency authorisation for access to o data held in a computer 'may authorise anything that a computer warrant may authorise'.[210]

While emergency authorisations will be permitted in a narrower set of circumstances than CA warrants, the scrutiny committees raised concerns about them. The PJCHR noted that the statement of compatibility does not address the proportionality of such authorisations.[211] The Scrutiny of Bills Committee questioned why they are required, given that law enforcement officers will be permitted to apply for CA warrants by telephone, fax, email or other form of communication if they believe it is impracticable to make an application in person (under **proposed section 27B**).[212]

206. *SD Act*, subsection 6(1) and section 6A. For example, for the AFP, an appropriate authorising officer is the Commissioner, a Deputy Commissioner or a senior executive AFP employee authorised by the Commissioner.
207. *SD Act*, subsections 28(1), 29(1) and 30(1); **proposed subsections 28(1A)**, **29(1A)** and **30(1A)**, inserted by **items 50**, **52** and **54**.
208. **Proposed subsections 28(1A)**, **29(1A)** and **30(1A)**, inserted by **items 50**, **52** and **54**.
209. **Items 51** (amending subsection 28(4)), **53** (amending subsection 29(3)) and **57** (inserting **proposed subsection 30(4)**).
210. **Item 59**.
211. PJCHR, *Human rights scrutiny report*, op. cit., pp. 46–47.
212. Scrutiny of Bills Committee, *Scrutiny digest*, op. cit., p. 33.

Issue: can telecommunications interception be authorised?

Based on statements by DoHA in a supplementary submission to the PJCIS, it appears that the Government intends for emergency authorisations to be able to permit limited interception in the same way as CA warrants.[213] However, while **proposed subsection 32(2A)** will allow the authorisation of 'anything that a computer warrant may authorise', emergency authorisations are not included in the definition of ***general computer access warrant*** to be inserted into the *TIA Act* by **item 120** of **Schedule 2**.[214] This creates uncertainty about whether or not interception may be permitted under an emergency authorisation.

The LCA recommended that interception not be permitted under an emergency authorisation.[215]

If interception is to be permitted under emergency authorisations, additional amendments to the *TIA Act* would be required to ensure that appropriate safeguards and protections apply.

Issue: can concealment activities be authorised?

The wording of **proposed subsections 32(2A)** and **27E(7)** (concerning concealment activities under a CA warrant during or after a warrant is in force) make it unclear whether an emergency authorisation may authorise the doing of things to conceal the fact that other things have been done under the authorisation. It could be argued that concealment activities may not be authorised, because concealment activities are authorised if any thing has been done to a computer under a CA warrant or under **subsection 27E(7)**, neither of which would apply where things were done under an emergency authorisation.

Approval of emergency authorisations

As is the case in relation to surveillance devices, an emergency authorisation for access to data held in a computer must be submitted to an eligible judge or nominated AAT member for approval within 48 hours of being given.[216] The eligible Judge or nominated AAT member may approve the authorisation if satisfied of certain matters, and only after considering particular matters, including the extent to which law enforcement officers could have used alternative methods and whether or not it was practicable in the circumstances to apply for a CA warrant.[217]

Extraterritorial operation of CA warrants

Part 5 of the *SD Act* sets out the extent to which surveillance devices may operate outside Australia, and the associated approval required. **Items 78–87** of **Schedule 2** of the Bill will amend Part 5 to make similar provision in relation to CA warrants.

If it becomes apparent before a CA warrant has been issued that there will be a need to access data held in a computer in a foreign country (or on a vessel or aircraft that is registered in another country and is outside Australia's territory) to assist in an investigation of a ***relevant offence***, the

213. DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 6.
214. The definition of ***general computer access warrant*** that will be inserted into the *TIA Act* states that it means a warrant issued under section 27C of the *SD Act*.
215. LCA, Submission to PJCIS, op. cit., p. 40.
216. *SD Act*, subsections 6(1) and 33(1), in conjunction with the amendments in **items 50–77** of **Schedule 2**.
217. *SD Act*, section 34 as amended by **items 63–68** of **Schedule 2**; **proposed subsections 35A(1)–(3)**, inserted by **item 76**. What the eligible Judge or nominated AAT member may order if the authorisation is approved or not approved is set out in **proposed subsections 35A(4)–(6)** (equivalent to subsections 35(4)–(6) of the *SD Act*).

eligible Judge or nominated AAT member must not permit that access unless he or she is satisfied that the access has been agreed to by an ***appropriate consenting official*** in the foreign country.[218]

If it becomes apparent after a CA warrant has been issued that such access will be required, the warrant will be taken to permit that access only if it has been agreed to by an appropriate consenting official.[219]

However, there will be several exceptions, among them, in circumstances where the person or each of the persons responsible for executing the warrant will be physically in Australia and the location where the data is held 'is unknown or cannot reasonably be determined'.[220]

Use, communication, publication and protection of information obtained under a CA warrant (other than information obtained by intercepting a communication)

Division 1 of Part 6 of the *SD Act* sets out restrictions on the use, communication and publication of information obtained from the use of a surveillance device or tracking device under the Act (referred to as ***protected information***). **Items 88–97** of **Schedule 2** will amend that Division so that information obtained from a CA warrant or emergency authorisation for computer access is also ***protected information*** and subject to those same restrictions. The exception to this will be information obtained under a CA warrant by intercepting a communication, which will instead by dealt with under the *TIA Act* (see further below under 'Use and protection of interception information …').[221] Amongst other things, this will mean that:

- the offences in section 45 of the *SD Act* for unauthorised use, recording, communication or publication of ***protected information*** and
- the obligations on agencies to keep ***protected information*** securely and to destroy records once no longer required in section 46

will apply to information obtained from a CA warrant or emergency authorisation for computer access (other than information obtained by intercepting a communication).

Section 47 of the *SD Act* makes provision for the protection of information that could reveal details of surveillance device technologies or methods in proceedings before a court, tribunal or Royal Commission. **Item 97** will insert **proposed section 47A** to make equivalent provision in relation to the protection of information that could reveal details of computer access technologies or methods. ***Computer access technologies or methods*** will mean technologies or methods relating to:

- the use of a computer, a telecommunications facility, any other electronic equipment or a data storage device for the purpose of obtaining access to data held in the computer or
- adding, copying, deleting or altering other data in a computer, if doing so is necessary to obtain access to data held in the computer

---

218. **Proposed subsection 43A(1)** of the *SD Act*, inserted by **item 87** of **Schedule 2**. **Proposed subsection 43A(2)** makes provision in relation to emergency authorisations. ***Appropriate consenting official*** will mean an official of the relevant foreign country having authority in that country to give that consent (**item 78**).
219. **Proposed subsection 43A(3)**, inserted by **item 87** of **Schedule 2**.
220. **Proposed subsection 43A(4)** of the *SD Act*, inserted by **item 87** of **Schedule 2**. See also **proposed subsections 43A(5)** and **(6)**.
221. **Item 88** will amend the definition of ***protected information*** in subsection 44(1) of the *SD Act* so that it includes any information obtained from access to data under a CA warrant or emergency authorisation, other than ***general computer access intercept information*** (which will mean information obtained under a CA warrant by intercepting a communication passing over a telecommunications system: **item 39** of **Schedule 2**, amending subsection 6(1) of the *SD Act* and **item 120**, amending subsection 5(1) of the *TIA Act*).

where the technologies or methods have been, or are being, deployed to give effect to a CA warrant or emergency authorisation for computer access.[222]

Use of information where control order is later declared void

Section 65B of the *SD Act* makes provision for how information obtained under a surveillance device may be dealt with if a warrant was issued on the basis that an interim control order was in force and a court subsequently declares that order to be void. It limits, but does not prevent, the use of such information.[223] **Item 119** will amend section 65B so that information obtained under a CA warrant may be dealt with in the same way. If an interim control order is declared void, a person will still be able to adduce the information as evidence in a proceeding; or use, communicate or publish the information; in certain circumstances.[224]

The Scrutiny of Bills Committee and the PJCHR raised concerns about the use of CA warrants to monitor compliance with control orders generally, and more specifically the ability to make use of information obtained after the interim control order to which a CA warrants related is declared void.[225]

Reporting and record-keeping

Division 2 of Part 6 of the *SD Act* sets out the reporting and record-keeping obligations of law enforcement agencies with respect to surveillance device warrants and authorisations and tracking device authorisations. **Items 98–111** will amend that Division to apply equivalent requirements in relation to CA warrants and emergency authorisation for computer access. This will mean that law enforcement agencies will be required to:

- submit a report to the Minister as soon as practicable after a warrant or authority expires that covers particular matters, including the use that has or will be made of evidence or information obtained by the access to data in achieving the purpose for which the warrant or authority was issued (except if issued in relation to a mutual assistance request) and, if the warrant or authority related to an investigation, the benefit to the investigation of the accessed data[226]
- notify the Commonwealth Ombudsman within six months of each CA warrant issued in relation to a control order, and provide a copy of the warrant[227]
- notify the Commonwealth Ombudsman as soon as practicable of any contraventions of certain provisions relating to CA warrants issued in relation to control orders or of conditions specified in such warrants[228]
- submit annual reports to the minister covering certain information for each financial year, including the number of arrests made wholly or partly on the basis of information obtained by access to data held in a computer, and the number of prosecutions for relevant offences commenced in which such information was given in evidence[229]

---

222. **Proposed subsection 47A(7)** of the *SD Act*.
223. Section 3ZZTC of the *Crimes Act* and section 299 of the *TIA Act* make similar provision for information (and in the case of the *Crimes Act*, also documents and things) obtained under warrants relating to interim control orders.
224. **Item 37** of **Schedule 2** will insert a definition of control order access warrant into subsection 6(1) of the *SD Act*.
225. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., pp. 39–42; PJCHR, *Human rights scrutiny report*, op. cit., pp. 42, 50–51.
226. **Proposed subparagraphs 49(2B)(b)(vi)–(ix)** and **proposed subsection 49(2C)** of the *SD Act*, inserted by **item 99** of **Schedule 2**. For the full list of matters to be included, see **proposed subsections 49(2B)** and **(2C)**.
227. Subsection 49A(1) of the *SD Act*, as amended by **item 100** of **Schedule 2**.
228. Subsection 49A(2) of the *SD Act*, as amended by **items 101–103** of **Schedule 2**.
229. **Proposed paragraphs 50(1)(g)** and **(i)**. For the full list of matters to be included, see section 50 of the *SD Act* and **items 105–107** of **Schedule 2**. The Minister must table these annual reports in each house of Parliament within 15 sitting days of receiving them (subsection 50(4)). Section 50A allows for the deferral of the inclusion of certain information relating to control orders in the tabled versions of annual reports.

- keep documents connected with CA warrants and emergency authorisations for computer access; and other records, including each use and communication of information obtained by access to data held in a computer and[230]
- keep details of each CA warrant and each emergency authorisation for computer access in a register.[231]

Issue: potential improvements to reporting and record-keeping requirements

There are several ways in which the reporting and record keeping requirements could be amended to provide greater transparency about CA and surveillance device warrants and emergency authorisations and aid the Commonwealth Ombudman's inspection role.[232] In particular consideration could be given to:

- requiring law enforcement agencies to report on and keep records about:
  - each time telecommunications interception took place under a CA warrant
  - each time action was taken to conceal the fact that something was done in relation to a computer under a CA warrant or **proposed subsection 27E(7)**[233]
  - if interception and/or concealment activities will be permitted under emergency authorisations for computer access, the above details in relation to such authorisations
  - each time concealment action was taken after the expiry of the warrant, and each time it was taken more than 28 days after the expiry of the warrant and
- requiring annual reports under section 50 of the *SD Act* to include all of the required details separately for surveillance device warrants and emergency authorisations and CA warrants and emergency authorisations for computer access. Section 50 as amended by the Bill will require some matters to be reported on separately by type of power (surveillance device or computer access), but permit much of the information, such as the number of applications for warrants and authorisations, the number of warrants and authorisations issued and the purposes for which warrants and authorisations were sought, to be provided in aggregate.[234]

Issue: no compensation for unlawful computer access

Section 64 of the *SD Act* provides that the Commonwealth is liable to pay compensation to a person for loss or injury resulting from the unlawful use of a surveillance device by a Commonwealth law enforcement agency. The Bill would not amend this section or insert an equivalent provision to also cover unlawful computer access. The Commonwealth Ombudsman and the LCA recommended that such a change should be made.[235] DoHA stated that the Government is considering whether to adopt such an amendment.[236]

Assistance orders under the SD Act

Item 114 will insert **proposed section 64A** into the *SD Act*. **Proposed subsection 64A(1)** will allow a law enforcement officer to apply to an eligible Judge or a nominated AAT member for an order

230. Section 51 of the *SD Act*, as amended by **item 108** of **Schedule 2**; **proposed paragraphs 52(1)(e)** and **(f)**. For the full list of other records to be kept, see section 52 of the *SD Act* and **items 109** and **110** of **Schedule 2**.
231. Section 53 of the *SD Act*, as amended by **item 111**.
232. The Commonwealth Ombudsman's inspection role and the powers in fulfilling it are set out in Division 3 of Part 6 of the *SD Act*. The Commonwealth Ombudsman is required to inspect the records of law enforcement agencies to determine the extent of their compliance with the *SD Act* and report to the Minister the results of those inspections every six months. The Minister must table these reports in each house of Parliament within 15 sitting days of receiving them.
233. Reporting on concealment activities was recommended by the Commonwealth Ombudsman: Commonwealth Ombudsman, Submission to PJCIS, op. cit., p. 6.
234. Section 50 of the *SD Act* as amended by the Bill would allow aggregate reporting of the matters specified in paragraphs 50(1)(a)–(b) and (d)–(f), and require disaggregated reporting of the matters in **proposed paragraphs 50(1)(g)–(i)**.
235. Commonwealth Ombudsman, Submission to PJCIS, op. cit., p. 7; LCA, Submission to PJCIS, op. cit., p. 47.
236. DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 8.

requiring a specified person to provide information or assistance that is reasonable and necessary to allow the officer to:

- access data held in a computer that is the subject of a CA warrant or emergency authorisation for computer access
- copy data held in such a computer to a data storage device and/or
- convert into documentary form or another form intelligible to the officer data that is held in a computer that is the subject of a CA warrant or emergency authorisation for computer access, or in a data storage device to which it was copied under the proposed subsection.

These orders will be similar to those that may be issued by magistrates to compel persons to assist officers to obtain access to data under search warrants, under section 3LA of the *Crimes Act* and section 201A of the *Customs Act*. **Schedules 3** and **4** of the Bill will amend those sections, including the penalties that apply for failing to comply with an order.

Purpose-related threshold for issue

As with CA warrants and emergency authorisation for computer access, the thresholds for issue will differ depending on the purpose for which the relevant warrant or authorisation was issued. For a warrant or authorisation issued in relation to an investigation of a relevant offence, an eligible Judge or a nominated AAT member may grant the order if he or she is satisfied that there are 'reasonable grounds for suspecting that access to data held in the computer is necessary in the course of the investigation for the purpose of enabling evidence to be obtained' of the offence or the identity or location of the offender.[237] This is equivalent to the purpose-related threshold for applying for or granting a CA warrant in relation to an investigation of a relevant offence.[238] The thresholds for orders in relation to warrants or authorisations issued for other purposes (recovery orders, mutual assistance authorisations, integrity operations and control orders) also mirror the thresholds for applying for a warrant or authorisation.[239]

Persons who may be specified

The person specified in an order may be:

- the owner or lessee of the computer or data storage device
- an employee of, or person engaged under a contract for services by, the owner or lessee
- a person who uses or has used the computer or device
- a person who is or was a system administrator for the system including the computer or device
- if the warrant or emergency authorisation relates to investigation of a relevant offence, a mutual assistance authorisation or loss of evidence, a person reasonably suspected of having committed the relevant offence/s
- if the warrant relates to an integrity operation, the staff member in relation to whom information on integrity, location or identity is sought or
- if the warrant relates to a control order, the subject of the control order.[240]

Such a person may only be specified in an order if the eligible Judge or nominated AAT member is satisfied that he or she has relevant knowledge of either the computer or device, or a computer

237. **Proposed paragraphs 64A(2)(a)–(c)**.
238. **Proposed paragraphs 27A(1)(c)** and **subsection 27C(1)(a)**.
239. **Proposed paragraphs 64A(3)(c)**, **4(a)**, **5(a)** and **6(a)** (assistance orders), **27A(3)(b)**, **4(b)**, **5(b)** and **6(b)** (applications for CA warrants) and **27C(1)(b)–(e)** (determining an application).
240. **Proposed paragraphs 64A(2)(d)**, **3(d)**, **4(b)**, **5(b)**, **6(b)** and **7(b)**.

network of which it forms or formed a part; or measures applied to protect data held in the computer or device.[241]

Offence for contravening an order

It will be an offence under **proposed subsection 64A(8)** for a person subject to an order and capable of complying with a requirement it contains to intentionally fail to do so.[242] The maximum penalty for an individual will be imprisonment for ten years, a fine of up to 600 penalty units (currently $126,000), or both.[243] The maximum penalty for a corporation will be a fine of 3,000 penalty units (currently $630,000).[244]

Issues raised in relation to assistance orders

The Scrutiny of Bills Committee, the PJCHR and some stakeholders had concerns about the proposed assistance orders and associated offence. The PJCHR and BSA noted the broad range of persons who might be compelled to provide assistance, and the breadth of what might be considered relevant knowledge.[245] The Scrutiny of Bills Committee, the AHRC and the LCA questioned whether the proposed penalties are appropriate, with the Committee and the AHRC noting the limited justification provided in the Explanatory Memorandum for the penalty in proposed **subsection 64A(8)** of the *SD Act* and increases to penalties for similar offences in the *Crimes Act* and *Customs Act* in **Schedules 3** and **4** of the Bill respectively.[246] The justification provided relates to instances where the person subject to an assistance order is the person being investigated for an offence.[247] However, other individuals and organisations may also be compelled to provide assistance under an order.

The Scrutiny of Bills Committee and some stakeholders were concerned about the possible impact of the proposed orders on the privilege against self-incrimination.[248] However, DoHA considered that assistance orders do not engage this privilege on the basis that such orders:

> … [do] not compel a person to confess guilt or provide evidence against interest. Assistance orders merely allow law enforcement the ability to search a device. This is not dissimilar from a search warrant executed on a premises where there is no argument that the right is not engaged. Assistance orders do not compel an individual to go into their device and disclose information or documents. It simply provides an avenue for law enforcement and national security agencies to lawfully gain access to that device, so that a lawful search of the device may be conducted as necessary.[249]

---

241. **Proposed paragraphs 64A(2)(e)**, **(3)(e)**, **(4)(c)**, **(5)(c)**, **(6)(c)** and **(7)(c)**.
242. For an offence to be made out, the prosecution would need to prove that a person: knew or was reckless as to whether they were subject to an assistance order under **proposed section 64A**, knew or was reckless as to whether they were capable of complying with a requirement in the order, intentionally omitted to do an act; and knew or was reckless as to whether that omission contravened the requirement (this explanation takes account of the application of default fault elements under section 5.6 of the *Criminal Code*). Note that where recklessness is the fault element, proof of intention, knowledge or recklessness will satisfy that fault element: *Criminal Code*, subsection 5.4(4).
243. **Proposed subsection 64A(8)**; *Crimes Act*, section 4AA (value of a penalty unit).
244. Ibid; *Crimes Act*, section 4B (corporate multiplier).
245. PJCHR, *Human rights scrutiny report*, op. cit., pp. 54–57; BSA, Submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 48], 12 October 2018., pp. 18–19.
246. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., pp. 45–47; AHRC, Submission to PJCIS, op. cit., pp. 75–77; LCA, Submission to PJCIS, op. cit., p. 45.
247. Explanatory Memorandum, pp. 117 (*SD Act*; states that the penalty is consistent with the amended penalty under the *Crimes Act*), p. 133 (justification for penalty in the *Crimes Act*), p. 139 (justification for penalty in the *Customs Act*).
248. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., p. 47; LCA, Submission to PJCIS, op. cit., pp. 45–47; AHRC, Submission to PJCIS, op. cit., pp. 77–80; Hochstrasser, Submission to PJCIS, op. cit., pp. 1–3; Civil Society, Submission to PJCIS, op. cit., p. 33.
249. DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 13.

The PJCIS was presented with the argument, in a submission from academic Daniel Hochstasser, that an express abrogation of the privilege is preferable:

> The solitary purpose of a statutory power to obtain an assistance order is to enable law enforcement officials to gain access to otherwise inaccessible encrypted material. To allow the recipient of an assistance order to refuse to comply with that order on the basis that to do so would infringe the privilege would render the order largely impotent. Despite this outcome, however, for purposes of certainty and consistency with State legislation it is preferable that the granting of a power to apply for an assistance order is accompanied by the express abrogation of the privilege against self-incrimination.[250]

Use and protection of intercept information obtained under the ASIO Act and the SD Act

Items 120–123, **124**, **125–126**, and **127–131A** will make amendments to the *TIA Act* consequential to the amendments the *ASIO Act* and the *SD Act* relating to CA warrants.

Definitions

Item 120 will insert definitions of ***ASIO computer access intercept information***, ***ASIO computer access warrant***, ***general computer access intercept information*** and ***general computer access warrant*** (one obtained under **proposed section 27C** of the *SD Act*) into subsection 5(1) of the *TIA Act*.

Item 121 will amend the definition of ***restricted record*** in subsection 5(1) of the *TIA Act* so that ***general computer access intercept information*** does not fall within the definition.

Item 122 will amend the definition of ***warrant*** in subsection 5(1) of the *TIA Act* so that in Chapter 2 of the *TIA Act*, except in Part 2–5, it will include a ***general computer access warrant*** and an ***ASIO computer access warrant***. The Explanatory Memorandum states that the reason for this amendment is to ensure that interception under one of those warrants is not prohibited by the *TIA Act*.[251] However, that will be achieved by the amendments to the operation of subsection 7(2) to be made by **item 123**.[252] Instead, this amendment will mean that some of the requirements for the AFP, ACIC and ACLEI to keep documents relating to warrants, and for the Commonwealth Ombudsman to inspect and report on those records, under Part 2–7 of the *TIA Act*, will apply to CA warrants issued under proposed section 27C of the *SD Act*.[253] Some of those requirements would duplicate what will be required under the *SD Act*, and to that extent, the application of those sections of the *TIA Act* to CA warrants appears to be unintended.

Dealing with intercepted information

Part 2–6 of the *TIA Act* sets out when information obtained by intercepting a telecommunication may be communicated and used, and when records may be made of such information.

Item 124 will insert **proposed sections 63AB** and **63AC**, which will set out how computer access intercept information may be dealt with. Under **proposed subsection 63AB(1)**, a person will be

---

250. Hochstrasser, Submission to PJCIS, op. cit., pp. 1–3.
251. Explanatory Memorandum, p. 119.
252. **Item 123** would insert **proposed paragraphs 7(2)(ba)** and **(bb)** into the *TIA Act* so that the general prohibition on interception of telecommunications will not apply to interception under subsections 25A(4), 27A(1) or 27E(2) or **proposed subsections 25A(8)**, **27A(3C)** or **27E(6)** of the *ASIO Act* or **proposed subsection 27E(7)** of the *SD Act*. There appears to be an error in **proposed paragraph 7(2)(bb)**, which refers to the subsection under which interception may be undertaken for the purposes of concealment, but not the subsection under which interception may be authorised in a CA warrant (**proposed subsection 27E(2)**).
253. See *TIA Act*, paragraphs 80(a) and (c) and sections 83 and 84.

permitted, for the purposes of doing a thing authorised by a ***general computer access warrant***, to communicate ***general computer access intercept information*** to another person; make use of, or make a record of, such information; and give such information in evidence in a proceeding. Communication, use and records of such information will also be permitted under **proposed subsection 63AB(2)** if the information relates or appears to relate to the involvement or likely involvement of a person in one or more of the following activities:

> (d) activities that present a significant risk to a person's safety;
>
> (e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);
>
> (f) activities that are, or are likely to be, a threat to ***security***;
>
> (g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of the Organisation [ASIO] or of ASIS, AGO or ASD (within the meanings of that Act);
>
> (h) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
>
> (i) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).[emphasis added]

Under the *TIA Act*, ***security*** takes the same meaning as in the *ASIO Act*.[254]

Proposed section 63AC makes equivalent provision for dealing with ***ASIO computer access intercept information***.

It will be an offence to deal with ***general computer access intercept information*** or ***ASIO computer access intercept information*** except as permitted under Part 2–6 and section 299 of the *TIA Act*.[255]

Issue: no exception in proposed section 63AC for the IGIS

The IGIS pointed out that one of the effects of **proposed section 63AC** and **item 125** will be to prohibit the disclosure to or by the IGIS of ***ASIO computer access intercept information***. The IGIS stated that she 'could not effectively oversee ASIO's warrant-based computer access activities without the ability to obtain, deal with and communicate' such information and accordingly, recommended the inclusion of an exception.[256] In support of that recommendation she stated:

> It is essential to the ability of IGIS to conduct oversight of ASIO's interception and related activities that the TIA Act continues to provide a clear exception for the voluntary disclosure of ***all forms*** of intercept information (however described) to, and by, IGIS officials for the purpose of those officials performing their functions or duties and exercising their powers as IGIS officials.

254. *TIA Act*, subsection 5(1) (see section 4 of the *ASIO Act*).
255. This is an existing offence that applies to prohibited dealings with intercepted information: *TIA Act*, sections 63 (prohibition on dealing in intercepted information or interception warrant information) and 105 (offence for contravention of section 7 or 63).
256. IGIS, Submission to PJCIS, op. cit., pp. 50–51 (quote taken from p. 51).

> As the Explanatory Memorandum to the Bill notes, 'it is almost always necessary for ASIO to undertake limited interception for the purpose of executing a computer access warrant'. The Human Rights Statement of Compatibility in the Explanatory Memorandum also identifies IGIS oversight of ASIO's computer access warrants as a key safeguard to ensure that the new powers authorised under those warrants are 'exercised lawfully, with propriety, and with respect for human rights'.[257][emphasis in original]

Issue: other dealings with computer access intercept information

The Explanatory Memorandum indicates that the Government intends that **proposed sections 63AB** and **63AC** set out the only exceptions to the general prohibition on dealing in computer access intercept information.[258] However, while items **125–126** and **127–131** will amend other sections in Part 2–6 of the *TIA Act* to limit dealings with computer access intercept information, it appears that:

- both types of computer access intercept information may be dealt with under section 63B (dealing in information by employees of carriers), 65A (employees of carriers communicating information to agencies), 66 (interceptor communicating information to officer who applied for warrant) and 72 (making a record for the purpose of permitted communication)
- ***general computer access intercept information*** might be able to be dealt with under sections 64 (dealing in connection with ASIO's or IGIS's functions) and 65 (communicating information obtained by ASIO)—while ASIO computer access intercept information will be excluded from these sections by **items 125** and **126**, general computer access intercept information (which could be communicated to ASIO under **proposed section 63AB**) will not and
- ***ASIO computer access intercept information*** might be able to be dealt with under section 67 (dealing for permitted purpose in relation to agency), because while general computer access intercept information will be excluded from this section by **item 127**, ASIO computer access intercept information (which could be communicated to an agency under **proposed section 63AC**) will not; and under section 75 (giving information in evidence where there is a defect in a warrant).

Issue: no requirement for destruction of interception information

Sections 79 and 79AA of the *TIA Act* require interception agencies to destroy ***restricted records*** when the records are not likely to be required for a ***permitted purpose***. Similarly, section 14 of the *TIA Act* requires ASIO to destroy records and copies of communications intercepted under Part 2–2 of the *TIA Act* when the Director-General of Security is satisfied that they are not required, or not likely to be required, by ASIO in connection with the performance of its functions or the exercise of its powers.

The Bill would not impose any destruction requirements on ASIO or on law enforcement agencies in relation to computer access intercept information. It is unclear why this should be the case.

Testing and developing interception technologies

Items 123A–123D, **124A**, **126AA** and **126A** will amend the *TIA Act* to allow carriers to assist security authorities in activities relating to developing or testing technologies or interception capabilities.

Currently only employees of a ***security authority*** are permitted to test or develop interception technologies. Amendments made to subsection 31(1), by **item 123A**, will allow a security authority

257. Ibid., p. 51. Footnote references have been omitted from this quotation and can be viewed in the source document.
258. Explanatory Memorandum, p. 121. No other exceptions are acknowledged in the Explanatory Memorandum.

to work with a carrier in order to test or develop interception technologies, as authorised by the Attorney-General. A request under amended subsection 31(1) will allow both employees of the security authority and employees of the carriers, if they are specified, to engage in activities relating to developing or testing technology or interception capabilities.

Enhanced search warrants: key issues and provisions in Schedules 3 and 4

Background

Schedules 3 and **4** of the Bill will expand powers under search warrants provided for by the *Crimes Act* and *Customs Act* respectively.

The Government has stated that current search warrants and assistance orders empowering police and ABF officials are outdated, as some provisions are limited to premises-based conditions.

An assistance order issued pursuant to a person-based warrant issued under the *Crimes Act* can compel a person to assist with access to a device that has been moved or seized. However, it cannot compel a person to provide assistance in-situ:

> Law enforcement can't compel that assistance in relation to a device, such as a mobile device, found on their [sic] person. [The measures] address this gap and [ensure] existing assistance orders reflect the prevalence of devices such as smart phones and tablets being carried by people.[259]

The *Customs Act* currently allows search warrants to be issued in relation to premises only, not persons.[260]

The proposed amendments would further facilitate the examination of computers and data storage devices, whether carried on a person or found on a premises, by addressing those gaps; and by allowing police to use computers and data storage devices located during a search, and other equipment, to access ***account-based data***.

Search warrants under the Crimes Act*—police powers*

A police search warrant issued in accordance with Division 2 of Part IAA of the *Crimes Act* must relate to gathering ***evidential material*** for the investigation of an offence.[261] The ordinary process for seeking a warrant involves the preparation of an affidavit that, inter alia, 'must outline information such as the type of offence being investigated, how the privacy of any person is likely to be affected, and why the warrant is necessary'.[262]

An ***issuing officer*** may issue a search warrant to an ***executing officer*** (a police constable) under the *Crimes Act* when satisfied that there are reasonable grounds for suspecting that a person has, or may have, ***evidential material*** in their possession, or that such material is or may be held at a ***premises***, within the next 72 hours.[263] An issuing officer may be a magistrate or justice of the peace, or other court employee who is authorised to issue search warrants.[264]

---

259. DoHA, Submission to PJCIS, op. cit., pp. 33–34.
260. *Customs Act 1901*, section 198.
261 *Crimes Act 1914*, sections 3C and 3E.
262. DoHA, Supplementary submission to PJCIS, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, [Submission no. 18.2], 23 October 2018 (question TOLA/007).
263. *Crimes Act*, Division 2 of Part IAA. (***Issuing officer***, ***executing officer***, ***evidential material*** and ***premises*** are all defined in section 3C.)
264. Ibid., section 3C.

Overview of Schedule 3 amendments

Definition of account-based data

The Bill introduces the term ***account-based data*** in recognition that, for the purposes of obtaining evidence, data stored on a device (***relevant data***) is distinguishable from data held in relation to a person associated with an ***account*** for an ***electronic service*** that is stored on an external server or cloud.[265]

Expansion of search warrant provisions

Schedule 3 will expand existing search warrant powers to access data and ascertain whether that data holds evidential value to a criminal investigation. The amendments will enable police to take additional actions to obtain:

- access to relevant data or ***account-based data*** from a device found in the course of searching a premises or the person specified in the warrant, or by other means and
- remote access to such data for the duration of the warrant through a ***telecommunications facility***, ***electronic service***, other electronic equipment or device.[266]

Proposed subsection 3F(2D) means that police executing a search warrant will not have to be physically present on warrant premises to access data relevant to their investigation.[267] **Proposed subsection 3F(2E)** has the same practical effect in the case of a warrant that is in force in relation to a person.

Actions permitted and duration of warrants

Actions proposed in the Bill to be permissible under a search warrant for the purposes of obtaining ***relevant data*** or ***account-based data*** include:

- using a device found in the course of the search, a telecommunications facility or other electronic equipment/data storage device to ascertain whether data accessed through these means is evidential material covered by the warrant
- adding, copying, deleting or altering other data held on the device found in the search to achieve that purpose, if necessary
- using any other computer or a ***communication in transit*** if necessary to access the data (and adding, copying, deleting or altering other data on that computer or in that communication in transit if necessary)
- copying data which has been obtained that is evidential material covered by the warrant, or that appears relevant to making a determination about the evidential value of data covered by the warrant and
- any other action reasonably incidental to the above.[268]

---

265. Explanatory Memorandum, p. 130, summarising **proposed section 3CAA** of the *Crimes Act*. For ***relevant data***, see **proposed subsection 3F(2A)**, inserted by **item 3** of **Schedule 3**.
266. **Items 2** and **3 of Schedule 3**, **proposed section 3CAA** and **proposed subsection 3F(2A)** of the *Crimes Act*; **item 1** of **Schedule 3**, **amending subsection 3C(1)** of the *Crimes Act* to incorporate terms under the *Telecommunications Act 1997* (***carrier***, ***communication in transit*** and ***telecommunications facility***), the *Enhancing Online Safety Act 2015* (***electronic service***) and under **proposed subsection 3CAA** (***account-based data***). Note that **proposed subsection 3CAA(3)** at **item 2** imports the meaning of ***account*** as defined in the *Enhancing Online Safety Act 2015.*
267. Explanatory Memorandum, p. 21.
268. **Item 3** of **Schedule 3**, **proposed subsections 3F(2A)** and **(2B)** of the *Crimes Act* (see also **proposed subsections 3F(2C)–(2E)**); **Item 6A** of **Schedule 3**, **proposed subsections 3K(5)** and **3K(6)** of the *Crimes Act* (see also **proposed subsections 3K(7)–(9)**). Some of these actions are already permitted in relation to data.

Things found in the course of a search under the warrant may be moved for the purposes of access, examination and processing in certain circumstances.[269] Currently, things may be moved for an initial period of 14 days, with extensions of up to seven days at a time.[270] The Bill would extend from 14 to 30 days the initial period for which devices may be taken for examination, while leaving the limit unchanged for other items.[271] It would also allow for extensions of time to examine devices of up to 14 days at a time.[272]

Assistance orders

A constable can currently apply to a magistrate for an assistance order in relation to a device at warrant premises, moved from warrant premises or a person, or seized.[273] The amendments would expand this to include devices found on a person but not (or not yet) removed or seized, so that an executing officer can require assistance on the spot.[274] This would mean that an executing officer could compel a person to assist by unlocking a device or authenticating a logon in the course of a frisk search, for example.[275]

Currently, a person who fails to comply with an assistance order commits an offence with a maximum penalty of two years' imprisonment.[276] The Bill will amend the offence provision to create two offences, contingent on the offence under investigation and to which the warrant relates.

A lesser offence will apply to a person subject to an assistance order who fails to assist by providing access to a device, where the offence to which the warrant relates is not a serious offence. The Bill will increase the maximum penalty for this lesser offence to five years' imprisonment, a fine of up to 300 penalty units (currently $63,000), or both.[277] The maximum penalty for a corporation would be a fine of 1,500 penalty units (currently $315,000).[278]

A higher 'aggravated' offence will apply where the warrant relates to a serious offence or a serious terrorism offence and the person subject to an assistance order—and capable of complying with a requirement it contains—fails to do so. The maximum penalty for an individual will be imprisonment for ten years, a fine of up to 600 penalty units (currently $126,000), or both.[279] The maximum penalty for a corporation will be a fine of 3,000 penalty units (currently $630,000).[280]

Search warrants under the Customs Act*—Australian Border Force powers*

An ABF search warrant issued in accordance with the *Customs Act* must relate to gathering ***evidential material*** for the investigation an offence.[281]

A ***judicial officer*** may issue a search warrant to an ***executing officer*** (an ABF officer) under the *Customs Act* when satisfied that there are reasonable grounds for suspecting that there is, or may

269. *Crimes Act*, subsection 3K(2).
270. Ibid., subsections 3K(3A), (3B) and (3D).
271. **Item 4** of **Schedule 3**, **amending subsection 3K(3A)** of the *Crimes Act*.
272. **Items 5** and **6** of **Schedule 3**, **amending subsections 3K(3B)** and **(3D)** of the *Crimes Act*.
273. *Crimes Act*, section 3LA.
274. **Item 8** of **Schedule 3**, **proposed subparagraph 3LA(1)(a)(ia)** of the *Crimes Act.*
275. Explanatory Memorandum, pp. 21–22, summarising proposed amendments to section 3LA of the *Crimes Act*.
276. *Crimes Act*, section 3LA.
277. Ibid., **proposed subsection 3LA(5)**.
278. *Crimes Act*, sections 4AA and 4B.
279. **Item 9** of **Schedule 3**, **proposed subsection 3LA(6)**.
280. *Crimes Act*, sections 4AA and 4B.
281 *Customs Act 1901*, section 198.

be, ***evidential material*** on or in a place, a conveyance or a container (***premises***) within the next 72 hours.[282] A ***judicial officer*** may be a magistrate or justice of the peace, or other court employee who is authorised to issue search warrants.[283]

Section 227AA of the *Customs Act* provides for an ABF officer to use, or give to another body to use, evidence of the commission of an offence under Part 9.1 or Subdivision B of Division 72 of the *Criminal Code*, which has been obtained when exercising powers under the *Customs Act*.[284]

Overview of Schedule 4 amendments

Expansion of search warrant provisions

The *Customs Act* currently allows search warrants to be issued in relation to premises only, not persons (though warrants relating to premises may authorise an ordinary or frisk search of a person at or near the premises in specified circumstances).[285]

The conditions under which search warrants relating to persons could be issued by virtue of the amendments in **Schedule 4** are based on the existing provisions relating to issuing premises-based warrants under the *Customs Act*.[286] In addition to allowing ABF officers to apply for search warrants in relation to persons, the amendments in **Schedule 4** will:

- expand powers exercisable under search warrants to obtain evidential material in the form of data from devices (mirroring some of the amendments in **Schedule 3**):
  - carried by the ***target person*** and/or seized from the person, including those moved to another place[287] or
  - found on or in a specified premises, or a ***recently used conveyance*** that a ***target person*** had operated or occupied within 24 hours before the search commenced, including those moved to another place[288]
- expand the application of assistance orders to include data storage devices as well as computers, and to include a broader range of people who have a connection to the device[289]
- introduce the tiered distinction between aggravated and lesser offences for failure to comply with an assistance order, along with equivalent increased penalties (as proposed in the **Schedule 3** amendments to the *Crimes Act*)[290] and
- extend the initial time for which computers and data storage devices may be moved for the purposes of access, examination and processing under the search warrant from 72 hours to 30 days, and provide for extensions of up to 14 days at a time.[291]

---

282. Ibid.
283. Ibid., subsection 183UA(1).
284. Part 9.1 of the *Criminal Code* deals with serious drug offences. Subdivision B of Division 72 of the *Criminal Code* deals with plastic explosives.
285. *Customs Act*, paragraphs 198(4)(b) and 199(1)(e).
286. *Customs Act*, section 198 (premises-based warrants) and **proposed section 199A** (person-based warrants).
287. Ibid., **proposed section 199B** of the *Customs Act* (authorisations relating to a person) and **item 8A** of **Schedule 4**, **proposed section 201AA** of the *Customs Act*.
288. **Item 4A** of **Schedule 4**, **proposed subsection 199(4A)** (authorisations relating to premises); **item 8A of Schedule 4**, **proposed section 201AA** of the *Customs Act*. See also **item 1** of **Schedule 4**, amending subsection 183UA(1) (definition of ***recently used conveyance***, which is tied to a ***target person*** under **proposed section 199B**).
289. **Items 9** and **13** of **Schedule 4**, amending paragraphs 201A(1)(a), (b) and (c) and paragraph 201A(2)(b). For example, an assistance order might specify a person who has been or is a system administrator for the device under **proposed subparagraph 201A(2)(b)(vi)**.
290. **Item 18** of **Schedule 4**, **proposed subsections 201A(3)** and **(4)** of the *Customs Act*.
291. **Items 6**, **7** and **8** of **Schedule 4**, amending subsections 200(3A) and (3B) and inserting **proposed subsection 200(3D)** of the *Customs Act*.

Actions permitted and duration of warrants

Actions that will be permitted under either a premises-based warrant or a person-based warrant are similar to those permitted under the *Crimes Act* as amended by **Schedule 3** (however, search warrants under the *Customs Act* will not permit access to account-based data).[292] In addition, the amendments in **Schedule 4** will permit an officer executing a person-based search warrant to record fingerprints or take forensic samples from devices in possession of the ***target person***.[293] Police already have these powers for search warrants issued under the *Crimes Act*.[294]

Issues common to proposed amendments under Schedules 3 and 4

The extensive information-gathering capability facilitated through the expansion of search warrant powers has raised concern among stakeholders about what restrictions will be applicable to information obtained through access to personal devices. For example, stakeholders considered that the amendments and explanatory materials could be supplemented with:

- elaboration and/or amendments addressing the privacy impact of the provisions on third parties (for example, under the power to access information associated with an online account through the inclusion of the definition of ***accounts-based data***)[295] and
- a statement of position on the possibility of mutual assistance in criminal matters provisions being invoked by the request of a foreign government for Australian assistance (especially if this were to relate to the enforcement of foreign law that might result in the death penalty).[296]

In addition, the President of the Senate wrote to the PJCIS about concerns (as outlined in relation to **Schedule 2** CA warrants) that the exercise of remote access powers under warrant may have an effect on potential claims of parliamentary privilege. The President suggested that the proper protection of privileged material in Parliament is an issue that requires resolution, whether before the Bill is passed or afterwards.[297]

As has been noted in relation to the proposed introduction of assistance orders under the *SD Act* in **Schedule 2**, the scrutiny committees and some stakeholders have raised concerns about the proportionality of the proposed penalties for non-compliance and the potential impact on the privilege against self-incrimination.[298] Related concerns are:

- the gravity of charges that may be laid against persons who are unable to comply due to their circumstance (through inability to recollect relevant authentication credentials, for example)[299] and
- the use of an assistance order for a 'collateral purpose' (whereby information is subsequently used as evidence in criminal proceedings that do not involve prosecution for the offence for which the warrant was originally obtained).[300]

---

292. **Item 4A** of **Schedule 4**, **proposed subsection 199(4A)** (authorisations relating to premises); **Item 5** of **Schedule 4**, **proposed section 199B** of the *Customs Act* (authorisations relating to a person).
293. **Item 5** of **Schedule 4**, **proposed subparagraphs 199B(1)(b)(ii)** and **(iii)** of the *Customs Act*.
294. *Crimes Act*, subparagraphs 3F(1)(b) and 3F(2)(b).
295. PJCHR, *Human rights scrutiny report*, op. cit., p. 57 and pp. 64–70; LCA, Submission to PJCIS, op. cit., p. 49; AHRC, Submission to PJCIS, op. cit., pp. 62–64.
296. LCA, Submission to PJCIS, op. cit., p. 49. (This concern also relates to recommendations made about **Schedule 2** amendments in the same submission.)
297. Ryan, Submission to PJCIS, op. cit.
298. See 'Assistance orders under the SD Act' above.
299. Civil Society, Submission to PJCIS, op. cit., pp. 32–33 (the concerns expressed in this submission were framed in terms of the Schedule 3 proposal only.)
300. Hochstrasser, Submission to PJCIS, op. cit., pp. 4–7.

ASIO assistance powers: key issues and provisions in Schedule 5

Voluntary assistance to ASIO

Overview of voluntary assistance provisions

The *ASIO Act* does not currently include any express provision relating to voluntary assistance to the organisation. **Proposed section 21A** of the *ASIO Act* will introduce civil liability protections for persons or bodies who, under certain circumstances:

- provide voluntary assistance at the request of the ASIO Director-General or
- make unsolicited disclosures of information to ASIO.[301]

The type of voluntary assistance that ASIO might request of a person or body is described, broadly, as conduct.[302] The type of assistance that might be unsolicited is also described as conduct; however, it is more narrowly constructed with reference to giving information or documentation to ASIO (or copying documents and giving copies to ASIO) under the reasonable belief that the conduct is likely to assist ASIO in the performance of its functions.[303]

The civil liability protections would not apply if the person/body engaging in either form of conduct were to commit an offence under Commonwealth, state or territory laws; nor in the event of the conduct resulting in significant property loss or damage.[304] The Director-General would be able to request assistance from a person or body if satisfied, on reasonable grounds, that it would assist ASIO to perform its functions.[305] He or she would also be permitted to enter into a contract or agreement for such assistance.[306] The Director-General would be able to delegate his or her functions to a senior position-holder.[307]

Issues raised in relation to voluntary assistance

The IGIS submission to the PJCIS inquiry described the new provision as 'a significant departure from the existing process of granting statutory immunities'.[308] The Scrutiny of Bills Committee noted that the explanatory materials are silent on the justification of the civil liability protection.[309]

Unclear application and mechanisms to facilitate oversight

The *ASIO Act* currently provides for the Attorney-General to confer protection from civil or criminal liability—under a law of the Commonwealth, state or territory—for individuals engaged in authorised ***special intelligence conduct*** under Division 4 of Part III.[310] Conduct in relation to a ***special intelligence operation*** is carried out under authorisation of the Attorney-General, which may only be granted on grounds related to matters stipulated in the statute.[311]

---

301. **Item 2** of **Schedule 5**, **proposed section 21A** of the *ASIO Act*.
302. **Proposed subsection 21A(1)**.
303. **Proposed subsection 21A(5)**.
304. **Proposed subparagraphs 21(A)(1)(d)** and **(e)** and **21(A)(5)(c)** and **(d)**.
305. **Proposed paragraphs 21A(1)(a)** and **(b)** and **subsection (2)**.
306. **Proposed subsection 21A(4)**.
307. **Item 1**, **proposed subsection 16(1A)**. ***Senior position-holder*** is defined in section 4 of the *ASIO Act* to mean an ASIO employee or affiliate who holds or is acting in an ASIO position known as Coordinator; or equivalent to, or higher than, a position occupied by an SES employee.
308. IGIS, Submission to PJCIS, op. cit., p. 51.
309. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., p. 49.
310. *ASIO Act*, section 4 and section 35K.
311. Ibid., section 35C.

The amendment to the *ASIO Act* under **item 2** of **Schedule 5** is distinctly different, in that a request for voluntary assistance does not require a ministerial authorisation. In this regard, it is more like the new regime for TARs proposed in **Schedule 1** amendments to the *Telecommunications Act*. Unlike the proposed TAR regime, however, the requisite procedural documentation of a request under **proposed subsection 21A(3)** is minimal: the Director-General must make a written record of the request within 48 hours of it having been made. The request itself may be made orally or in writing; there are no additional statutory conditions:

- pertaining to the form, content or duration of a request or
- for a person to be notified that rendering assistance in accordance with the request is voluntary.[312]

The IGIS suggested that the Bill could impose statutory conditions for making a request—including consideration of the proportionality of any immunity conferred through rendering assistance—and that records and reporting arrangements ought to be made explicit in the Bill to ensure that conduct arising from the new provision may be assessed against standards of propriety and legality as required under the *ASIO Act*.[313] The AHRC recommended that such requests be subject to a defined period of maximum duration, so as not to become a 'standing requests'.[314]

A further point of distinction from the civil liability protection currently in the statute is that **proposed section 21A** does not sit in the context of ASIO's special powers, but in the context of ASIO's general functions. Unlike the technical assistance that may be requested of industry under the **Schedule 1** amendments, the types of assistance that might be requested or accepted under **proposed section 21A** are not listed.[315]

Voluntary compliance with a request for assistance under **proposed subsection 21A(1)**—and, in particular, a contract, agreement or arrangement entered into under **proposed subsection 21A(4)**—may render a person or body an ***ASIO affiliate*** under section 4 of the *ASIO Act*, with the implication that IGIS oversight might extend to the conduct insomuch as it comprises the performance of certain of ASIO's statutory functions.[316] If this status is enlivened under the circumstances, the person or body may be afforded additional identity protections under section 92 of the *ASIO Act*, and may be obliged to cooperate with the IGIS with respect to oversight arrangements. The IGIS cautioned:

> If ASIO were to adopt a practice of using new subsection 21A(1) as the means by which persons become ASIO affiliates, the result would be that civil immunity could be conferred on a very broad class of persons.[317]

The Bill and its extrinsic materials do not detail whether ASIO would:

- be required to inform a person or body providing voluntary or unsolicited assistance that such conduct may invoke contingent obligations (to cooperate with the IGIS, for example) or protections or
- to otherwise ensure that the person or body subject to a request is clearly informed of their legal position with respect to compliance.[318]

---

312. **Proposed subsection 21A(2)**; **proposed Division 2** of **Part 15** of the *Telecommunications Act*, specifically **new section 317HAA**.
313. IGIS, Submission to PJCIS, op. cit., pp. 52–53 and 57.
314. AHRC, Submission to PJCIS, op. cit., p. 84.
315. See **item 7** of **Schedule 1**, **proposed section 317E** (listed acts or things). .
316. IGIS, Submission to PJCIS, op. cit., pp. 52–53 and p. 59.
317. Ibid., pp. 52–53.
318. See, for example, IGIS, Submission to PJCIS, op. cit., p. 57.

The broad concept of conduct under **proposed section 21A** was highlighted by the PJCHR, which noted in its report that 'it is difficult to assess what rights this measure may engage and limit, and whether those limitations are legitimate for the purposes of international human rights law'.[319] The PJCHR's analysis noted that the Statement of Compatibility does not address the right to an effective remedy for parties affected by conduct covered by the new provisions.[320] The Scrutiny of Bills Committee sought the Minister's advice 'as to why it is considered necessary and appropriate to confer [civil liability] immunity … such that affected persons would no longer have a right to bring an action to enforce their legal rights'.[321]

Proposed subparagraphs 21A(1)(d) and **(e)** and **21A(5)(c)** and **(d)** are express limitations on the civil liability protections that affected persons could rely upon in pursuit of a legal remedy. The IGIS has suggested that these limitations would be enhanced by attaching reporting and notification requirements to uses of the immunity and that the limitations might be expanded to exclude:

- conduct that results in significant economic or financial loss (for example, loss of income or a decrease in the market value of property) and
- negligence that results in physical or mental harm or injury.[322]

It is not clear whether any additional legal implications (such as a requirement to maintain confidentiality) may arise through unsolicited assistance under **proposed subsection 21A(5)**.

Proposed subsection 21A(8) would enable the Director-General of Security, or a delegate, to certify factual information in writing pertaining to their satisfaction that voluntary or unsolicited assistance was likely to assist ASIO in its functions. This certificate could then be produced as evidence in any proceedings that relate to such assistance and, according to **proposed subsection 21A(9)**, would be admitted as prima facie evidence of the facts certified.

The Scrutiny of Bills Committee sought the Minister's advice about the justification for provisions enabling senior departmental officials to issue evidentiary certificates and the circumstances intended to be covered 'including the nature of any relevant proceedings'. The underlying concern that the Committee expressed was that the effect of these in proceedings might be to reverse the evidential burden of proof on any party seeking to challenge the lawfulness of actions covered by a certificate, given that party would need to rebut or dispute facts in the certificate with limited information about the validity, extent and/or intention of conduct that had had an impact on that person's rights.[323]

Issue: potential overlap between Schedule 1 TARs and Schedule 5 assistance powers

The AHRC highlighted the potentially broad application and overlap of the **Schedule 5** regime with the regime applicable to **designated communications providers** under the amendments in **Schedule 1**.[324] The IGIS also underscored the interaction of items in **Schedule 5** with the amendments proposed in **Schedule 1**, with the effect that:

> … intelligence agencies will potentially have multiple grounds of statutory immunity from civil and criminal liability that they could apply to communications providers who perform functions for them, which apply different thresholds and are subject to different conditions and limitations.

319. PJCHR, *Human rights scrutiny report*, op. cit., pp. 70–71.
320. Ibid.
321. Scrutiny of Bills Committee, *Scrutiny digest*, op. cit., p. 49.
322. IGIS, Submission to PJCIS, op. cit., pp. 53–54.
323. Scrutiny of Bills Committee, *Scrutiny digest*, op. cit., pp. 42–45.
324. AHRC, Submission to PJCIS, op. cit., p. 83.

> It is conceivable that, in some circumstances, agencies will have a choice about which type or types of statutory immunity they will engage in a particular operation.
>
> …
>
> For example, **in the case of ASIO**, there may be a choice between the issuing of a technical assistance request and a request under new s 21A(1) of the *ASIO Act* (Schedule 5) or obtaining an authorisation for the provider as a participant in a special intelligence operation; or compelling assistance under a technical assistance notice or obtaining an order under new s 34AAA of the *ASIO Act* (Schedule 5).[325] [emphasis added]

These same stakeholders have emphasised that the relationship between proposed voluntary assistance requests and the existing ASIO warrant and authorisation regimes is nowhere expressly addressed in the Bill itself, or in the explanatory materials.[326]

Orders to compel assistance to ASIO

Background

The *ASIO Act* currently includes provisions requiring persons, under warrant, to assist ASIO with its intelligence gathering function under special powers relating to terrorism offences provided in Division 3 of Part III.[327] These existing provisions enable ASIO to question or to detain an individual for questioning under exceptional circumstances to obtain intelligence directly from that person.[328]

The Government has stated that the new coercive powers measures in the Bill are 'directed towards the legitimate objective of ensuring':

> …that ASIO can give effect to warrants which authorise access to a device. ASIO's inability to access a device [due to evolving technologies and the prevalence of encryption] can frustrate operations to protect national security. The measures are a reasonable and proportionate response to the challenges brought about by new technologies, including encryption.[329]

Overview of new coercive powers

The amendment proposed in **item 3** of **Schedule 5** would enable ASIO to compel assistance with its intelligence gathering though access to data in certain circumstances. The exercise of these special powers would be contingent on a warrant issued in accordance with:

- Division 2 of Part III (specifically, a computer access, surveillance device or search warrant)[330] or
- Division 3 of Part III (a questioning warrant or a questioning and detention warrant authorising the seizure of a device from the person specified in the warrant).

---

325. IGIS, Submission to PJCIS, op. cit., p. 7 (see also note 21 on that page).
326. AHRC, Submission to PJCIS, op. cit., pp. 83–84; IGIS, Submission to PJCIS, op. cit., pp. 54–55.
327. *ASIO Act*, Division 3 of Part III, Subdivision B (questioning warrants) and Subdivision C (questioning and detention warrants).
328. The coercive powers under Division 3 of Part III are subject to a sunset clause and are set to expire in September 2019, unless extended for a further period or replaced with new provisions (which are anticipated to be introduced into Parliament with sufficient time for inquiry and review prior to the expiry date): see PJCIS, *Review of ASIO's questioning and detention powers*, PJCIS, Canberra, March 2018. The coercive powers under **proposed Subdivision J** of **Division 2** of **Part III** do not have equivalent periodic review and sunset clause provisions to those under Division 3 of Part III.
329. DoHA, Submission to PJCIS, op. cit., pp. 38–39.
330. Relevant warrants are search warrants issued under section 25; computer access warrants issued under section 25A; surveillance device warrants issued under section 26; and warrants for the purpose of obtaining foreign intelligence within Australia issued under section 27A. Relevant authorisations are those issued under sections 27D (searches of premises or persons); 27E (computer access); and 27F (surveillance devices) in relation to identified person warrants.

Proposed Subdivision J of Division 2 of Part III of the *ASIO Act* will allow the Attorney-General, at the request of the Director-General of Security, to make orders requiring a person to assist ASIO with their execution of the warrant, or risk committing an offence if the person fails to comply with the order.

Proposed subsection 34AAA(1) will enable the Director-General to apply to the Attorney-General for an order that requires a specified person to provide information or assistance that is reasonable and necessary to allow ASIO to access, copy and/or convert into an intelligible form data held in or accessible from a computer or data storage device subject to or located under an ASIO warrant or authorisation, or seized under a search of a person conducted by a police officer under section 34ZB of the *ASIO Act*.[331]

The Attorney-General may grant an order if satisfied:

- on reasonable grounds, that the use of the special power will:
  - assist ASIO to access foreign intelligence in a manner authorised under a warrant in relation to premises, a person, a computer or an identified object and
  - enable ASIO to collect such intelligence in relation to a matter in the interests of Australia's national security, foreign relations or national economic wellbeing (determined on the basis of advice from the Defence Minister or the Foreign Affairs Minister),[332] or
- that there are reasonable grounds to suspect ASIO will be substantially assisted with collection of intelligence in accordance with the *ASIO Act* in respect of a matter important to security; and
- the specified person:
  - is reasonably suspected of involvement in activities prejudicial to security or
  - has relevant knowledge of and means of access to a computer, device or computer network whereby such intelligence may be obtained (including owners or lessees and their employees or contractors; system administrators; or persons with shared use of a computer or device or computer network).[333]

An order thus issued would apply to a person:

- who is 'reasonably suspected of being involved in activity prejudicial to security'[334] or
- who holds a useful connection to a device or computer network subject to a warrant, by virtue of relevant knowledge of how to gain access to data linked to the purpose of that warrant.[335]

The measure has a potentially broad application to persons that turns on how ASIO determines suspicion of involvement in activities prejudicial to security. A person need not knowingly or intentionally be involved in such activities. DoHA explained in a submission to the PJCIS:

> Given the seriousness of potential acts that are prejudicial to security, it is critical that ASIO be able to compel assistance from persons suspected of involvement. There are many ways in which involvement may be made out, but these should be viewed through the lens that there are many people with relevant knowledge that can ensure the discovery and safe resolution of activities that represent a material threat to the Australian public.
>
> For example assistance can be sought from persons that are unintentionally acting as a conduit for activities that are prejudicial to security, or provide services to another person which enables them to

331. **Proposed subparagraph 34AAA(1)(a)(ix)** refers to something seized under section 34ZB, which provides for searching and strip searching persons detained under a warrant enabling special powers in relation to terrorism offences under Division 3 of Part III.
332. **Proposed paragraph 34AAA(2)(a)**.
333. **Proposed paragraphs 34AAA(2)(b)**, **(c)** and **(d)**.
334. Explanatory Memorandum, p. 27.
335. Ibid.

conduct activities that are prejudicial to security. Limiting this provision to those that are knowingly and intentionally involved in activities that are prejudicial to security may inhibit legitimate ASIO investigations and intelligence gathering and establish a critical gap.[336]

Proposed subsection 34AAA(4) will create an offence for a person who is subject to an order, capable of complying with a requirement of the order, and fails to do so. The maximum penalty for an individual would be imprisonment for five years, a fine of up to 300 penalty units (currently $63,000), or both. The maximum penalty for a corporation would be a fine of 1,500 penalty units (currently $315,000).[337]

In effect, these provisions would enable ASIO to compel, for example:

- the provision of a 'password, pin code, sequence or fingerprint necessary to unlock a phone subject to a section 25 warrant' or
- the assistance of 'a specialist employee of a premises subject to a section 25 warrant … to interrogate the relevant electronic database or use the relevant software so that [ASIO officers] can obtain a copy of particular records or files'.[338]

Proposed section 34AAA is similar to:

- assistance orders available to police under section 3LA of the *Crimes Act*, under which a constable—for the purposes of executing a search warrant—may apply to a magistrate for an order requiring a person to provide assistance accessing data held in or accessible from a computer or data storage device (and similar orders under the *Customs Act*),[339] and
- orders proposed under **Schedule 2** of the Bill in relation to computer access warrants for law enforcement agencies.[340]

The Explanatory Memorandum notes the similarity to the *Crimes Act* powers available to police where it explains that the intended effect is to enable 'ASIO to compel those who are able to provide ASIO with knowledge or assistance on how to access to data [sic] on computer networks and devices to do so'.[341] However, unlike the coercive powers for law enforcement upon which the new coercive intelligence power is modelled, **proposed section 34AAA** orders are made by a minister (the Attorney-General) rather than a judicial officer.

Issue: unclear implications for persons subject to a 34AAA order

The IGIS contrasted the issuing authority aspect of these regimes in its submission to the PJCIS inquiry, where the suggestion was put that **proposed section 34AAA** might benefit from amendment to subject its operation to additional safeguards for a person specified in an order.[342] The Scrutiny of Bills Committee noted that the search warrant amendments proposed under **Schedules 3** and **4** of the Bill have been introduced with safeguard provisions, highlighted in the

336. DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 19.
337. **Proposed subsection 34AAA(4)**. The five-year maximum penalty for an individual aligns with maximum penalties for non-compliance with ASIO's coercive powers under Division 3 of Part III of the *ASIO Act*, section 34L, but is lower than the proposed maximum penalties included in the Bill for non-compliance with assistance orders made under the *SD Act* (**proposed section 64A**, inserted by **item 114** of **Schedule 2**), and for non-compliance with assistance orders made under the *Crimes Act* and the *Customs Act* when the offence under investigation is a serious offence (**item 9** of **Schedule 3** and **item 18** of **Schedule 4** respectively).
338. DoHA, Submission to PJCIS, op. cit., p. 38.
339. *Crimes Act*, section 3LA; *Customs Act*, section 201A.
340. **Proposed section 27A** of the *SD Act* under **item 49** of **Schedule 2**. See discussion under 'Law enforcement computer access warrants under the *SD Act*' above.
341. Explanatory Memorandum, p. 145.
342. IGIS, Submission to PJCIS, op. cit., p. 65.

Government's statement of compatibility, such that a judicial officer or magistrate is the issuing authority for the coercive powers of law enforcement officers.[343]

Existing special powers safeguards in the *ASIO Act* would not extend to the new provisions under Division 2 of Part III. The reliance on the Attorney-General's ministerial authority is one aspect of the Bill that has drawn comment about further safeguards not being explicit in relation to ASIO's use of the provisions, prompting questions about how any implied safeguards might work in practice.[344] For example, multiple stakeholders posited a scenario that a person subject to such an order may be arrested on suspicion of the new offence under **proposed subsection 34AAA(4)** if the person attempts to leave a place where ASIO is requiring them to assist without first providing that assistance.[345] How this person might avail themselves of their legal rights in this scenario—for example, to contact a lawyer—remains unclear.

Other concerns about implications for persons identified for the purposes of an order made under **proposed section 34AAA** relate to:

- the specificity of classes of persons intended to be captured by **proposed subsection 34AAA(2)** (whether legal persons and/or natural persons)[346]
- the scope of potential application to persons specified under **proposed subparagraph 34AAA(2)(c)(i)** (whether a person reasonably suspected of involvement in activities prejudicial to security would need to be connected to the same security matter specified in the antecedent warrant)[347]
- the potential for interaction of the new special powers under Division 2 of Part III with the existing framework of coercive powers available under Division 3 of Part III (whether concurrent or consecutive use of either regime is contemplated, and what potential oppression might arise through being subject to multiple coercive powers)[348] and
- the procedural requirements under **proposed subsection 34AAA(3)** being applicable in a sub-set of circumstances and not uniformly to anybody compelled to assist.[349]

In addition to these concerns, the IGIS has raised the question of whether an order would engender liability for secrecy offences under subsection 18(2) and sections 18A and 18B of the *ASIO Act*; or liability for disclosure of 'inherently harmful information' under the new Division 122 of the *Criminal Code*.[350]

---

343. Scrutiny of Bills Committee, *Scrutiny digest*, 12, 2018, op. cit., p. 38. Explanatory Memorandum, p. 22, para. 105 (**Schedule 3**, requirement for a judicial officer); and p. 26, para. 127 (**Schedule 4**, requirement for a magistrate).
344. LCA, Submission to PJCIS, op. cit., pp. 54–55. The AHRC also contrasts the new Division 2 of Part III regime with the Division 3 of Part III provisions, stating: 'the new assistance order regime … does not make provision for a person to contact a lawyer or family member; there is no maximum period prescribed for the giving of assistance; there is no obligation on officers to explain the nature of the assistance order and what it requires; there is no obligation on officers to explain how to make a complaint to the IGIS or to challenge the making of the assistance order in court; there is no obligation to make an interpreter available if necessary; and there is no statutory obligation to treat the person humanely and with respect for their human dignity. … Particular consideration should be given to how assistance orders may impact on children': AHRC, Submission to PJCIS, op. cit., 81. See also IGIS, Supplementary submission to PJCIS, op. cit., [Submission 52.1], pp. 7–9.
345. IGIS, Submission to PJCIS, op. cit., p. 64; AHRC, Submission to PJCIS, op. cit., p. 80; LCA, Submission to PJCIS, op. cit., pp. 53–54. The Department's supplementary submission stated: 'The powers under section 34AAA to compel a specified person to assist ASIO are not contemplated to create the basis for the deprivation of liberty or inhumane treatment': DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 16. The IGIS suggested that the PJCIS consider 'whether the Bill contains adequate safeguards to ensure that the power cannot be exercised in a manner contrary to the stated intent': IGIS, Supplementary submission to PJCIS, op. cit., [Submission 52.1], p. 8.
346. AHRC, Submission to PJCIS, op. cit., p. 81; IGIS, Submission to PJCIS, op. cit., p. 60; LCA, Submission to PJCIS, op. cit., p. 52.
347. IGIS, Submission to PJCIS, op. cit., p. 61; LCA, Submission to PJCIS, op. cit., p. 52.
348. IGIS, Submission to PJCIS, op. cit., pp. 65–66; LCA, Submission to PJCIS, op. cit., pp. 54–55.
349. IGIS, Submission to PJCIS, op. cit., pp. 65–66; LCA, Submission to PJCIS, op. cit., pp. 54–55. (Limited application of the procedural requirements is based on the physical location of the device being on premises other than warrant premises.)
350. IGIS, Submission to PJCIS, op. cit., pp. 66–67.

For persons specified in an order, there is no statutory requirement imposed on ASIO to serve the order on that person or to notify them of conditions applicable to their compliance.[351] The IGIS contrasted the absence of such provisions in **Schedule 5** with provisions that govern the duration and compliance period for TARs, TANs and TCNs in **Schedule 1**.[352]

Issue: accountability and oversight

The unclear implications for persons compelled to provide assistance have led to a range of suggestions that additional reporting and record-keeping requirements would enhance oversight and accountability in relation to the actions ASIO undertakes and information it obtains through the use of the new coercive power.[353]

Absent further statutory requirements and clarification about associated amendments to ministerial guidelines, the IGIS has said that overseeing ASIO's exercise of these extended computer access-related powers may be a challenge.[354] Requirements relating to form, record-keeping, discontinuance and destruction apply under general provisions relating to warrants in the *ASIO Act*.[355] None of these requirements are replicated under **proposed Subdivision J**.

DoHA explained:

> The Attorney-General must be satisfied that the [ability to compel assistance in relation to a device] is subject to an issued ASIO warrant. This means that the thresholds of the particular warrant have been met.[356]

The issue of a warrant, however, precipitates requirements beyond relevant threshold considerations—these requirements appear not to apply to the proposed new orders. For example, section 32 of the *ASIO Act* imposes certain record-keeping obligations on the Director-General of Security and the Attorney-General that the Bill does not modify to enable correlation of a **proposed section 34AAA** order with its antecedent warrant; nor does the Bill prescribe explicit obligations pertaining to the form of such an order (whether oral or written).[357]

Whereas actions taken under a relevant warrant must be reported to the Attorney-General, these requirements are not amended by the Bill to apply to orders.[358] Actions taken under a **proposed section 34AAA** order, while contingent on an antecedent warrant, are not captured by the existing reporting requirements for warrants.[359] The Department takes the view that existing safeguards and limitations would prevent the abuse of powers through activities authorised by an order, stating:

> Reporting requirements under the ASIO Act are mostly reserved for warranted activities. … It would not be in keeping with the existing regime for the assistance orders … to be subjected to mandatory reporting. The existing safeguards and limitations also prevents the use of assistance orders for arbitrary

---

351. IGIS, Submission to PJCIS, op. cit., p. 64.
352. Ibid.
353. Ibid., pp. 59–67; LCA, Submission to PJCIS, op. cit., pp. 52–53.
354. IGIS, Submission to PJCIS, op. cit., pp. 59–67. (See also the statement at pages 2–4 of this submission that sets out the concerns about Schedule 5 amendments in the context of the overall effect of amendments proposed in the Bill on the IGIS' ability to exercise its functions.)
355. *ASIO Act*, Subdivision H of Division 2 of Part III. Similar provisions are contained in Subdivision E of Division 3 of Part III with additional, specific limitations on the use of coercive powers under questioning and questioning and detention warrants.
356. DoHA, Submission to PJCIS, op. cit., p. 39.
357. IGIS, Submission to PJCIS, op. cit., p. 62. The Department has explained that **proposed subsection 34AAA(4)(b)** implicitly provides that 'a compulsory assistance order must be provided to the specified person in a form that ensures they are able to comply with the requirements in an order': DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 20.
358. *ASIO Act*, sections 34 and 34ZH.
359. IGIS, Submission to PJCIS, op. cit., p. 66.

reasons and ensures that this power is only used in specific circumstances, explicitly limiting the potential for major loss or damage or illegal conduct.[360]

The Bill does not extend the obligations concerning retention, destruction, handling and secondary use of information obtained under a warrant to information obtained under a **proposed section 34AAA** order. The handling of information obtained under a warrant is subject to limitations on its secondary use, and must be destroyed if no longer required for the purposes of the performance of functions or legitimate exercise of ASIO's statutory powers.[361] The IGIS points out that, while the Explanatory Memorandum contemplates the collection of sensitive information, including biometric information, 'where necessary to gain access to a computer', there is no explanation about how such information is subsequently governed under the *ASIO Act*.[362]

Concluding comments

The Bill will introduce more capability for intelligence and law enforcement agencies to disrupt and investigate criminal activity and threats to national security, including organised crime and terrorism. The use of industry to assist, by either a request or an order, in the decryption of communications, will help agencies to keep up with the range of technology that may be used to facilitate criminal activity. The Bill will further expand the capabilities of security and law enforcement agencies to access information and data at points where it may not be encrypted, through search and computer access warrants, and the use of assistance orders. The Bill will also enable persons to voluntarily provide assistance to ASIO with protection from civil liability.

There are several aspects of the Bill that may be drafted more broadly than would be required to meet its stated objectives. Amendments to address those aspects and provide greater clarity about the scope of proposed powers would be welcomed by industry and civil society stakeholders.

The safeguards and accountability mechanisms that sit alongside the expanded powers could also be strengthened, and consideration given to a statutory review of the amendments in the Bill within a certain period of their commencement. Such a review would maintain the ability of Parliament to keep abreast of the utility and efficacy of the enhanced capabilities so that any future debate on proposals to refine or change these powers may be well informed.

360. DoHA, Supplementary submission to PJCIS, op. cit., [Submission 18.3], p. 19.
361. *ASIO Act*, section 31.
362. IGIS, Submission to PJCIS, op. cit., p. 63.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2500.